

Slack, Jessica

From: Slack, Jessica on behalf of PS Media Relations / Relations médias SP
Sent: December-22-11 4:40 PM
To: [REDACTED] s.19(1)
Subject: RE: question re press release

Rob,

Received. I will check on this for you, but an interview today will not be possible.
Jessica

-----Original Message-----

From: [REDACTED] s.19(1)
Sent: Thursday, December 22, 2011 4:34 PM
To: PS Media Relations / Relations médias SP
Subject: question re press release

Hi,

I'm a freelance journalist based in Victoria, BC, and I'd like to interview someone asap (as in, immediately), about the following press release:

<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.

I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.

thank you,

[REDACTED]

s.19(1)

Slack, Jessica

From: Slack, Jessica
Sent: December-22-11 5:04 PM
To: Champoux, Martin
Cc: Wilson, Barbara; Swift, Andrew
Subject: FW: question re press release

Martin, for discussion in the morning!

-----Original Message-----

From: Filipps, Lisa
Sent: Thursday, December 22, 2011 4:34 PM
To: Slack, Jessica
Subject: FW: question re press release

From: PS Media Relations / Relations médias SP
Sent: Thursday, December 22, 2011 4:34:00 PM (UTC-05:00) Eastern Time (US & Canada)
To: Swift, Andrew; Fergusson, Janis; Filipps, Lisa; McDonald, Jessica
Subject: FW: question re press release **s.19(1)**

From: [REDACTED]
Sent: Thursday, December 22, 2011 4:35:44 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: question re press release

Hi,

I'm a freelance journalist based in Victoria, BC, and I'd like to interview someone asap (as in, immediately), about the following press

release:

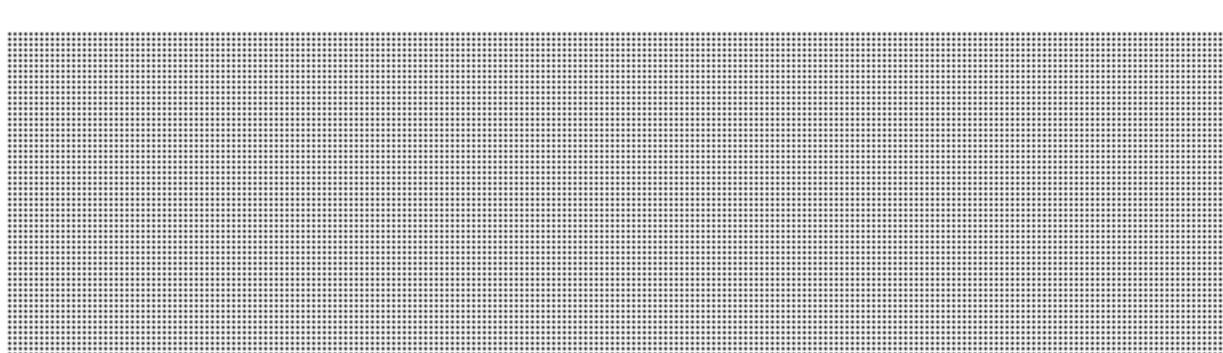
<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.

I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.

thank you,
Rob Wipond

s.19(1)



Slack, Jessica

From: Durand, Stéphanie
Sent: December-23-11 12:03 PM
To: Dick, Robert
Cc: Swift, Andrew; Champoux, Martin; Slack, Jessica; Wilson, Barbara
Subject: FW: question re press release

Hi Robert:

As discussed, here is the question from the reporter re a CCIRC product. Link is below.
We will need you and your team to clarify.
Martin will be following-up with you on best approach.

Stéphanie Durand
Director General, Communications | Directrice générale, Communications

Public Safety Canada | Sécurité publique Canada
269 Laurier, 18D-3600
Ottawa, Canada K1A 0P8
stephanie.durand@ps-sp.gc.ca
Telephone | Téléphone 613 991-2799
Facsimile | Télécopieur 613 993-7062
Government of Canada | Gouvernement du Canada www.PublicSafety.gc.ca | www.SecuritePublique.gc.ca

-----Original Message-----

From: Champoux, Martin
Sent: Friday, December 23, 2011 11:40 AM
To: Durand, Stéphanie
Cc: Swift, Andrew; Slack, Jessica; Wilson, Barbara
Subject: FW: question re press release

Stephanie

As discussed

We have received a media call from a freelance journalist in BC who wants an expert to explain to him in layperson's terms an Information Note published by CCIRC on 20 Dec 2011. See link for document in question.

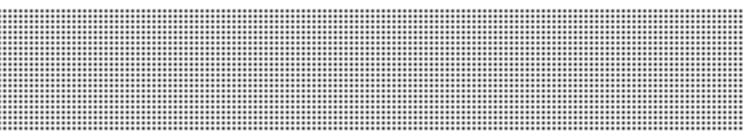
<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

I spoke with Andrew S. His recommendation is to offer, subject to proper approvals, a 10 minute background interview only. Should the journalist want a formal interview after this, one could be arranged at a later date again subject to approval.

Please let me know how you wish for us to proceed. Thank you

Martin

s.19(1)

From: 

Sent: Thursday, December 22, 2011 4:35:44 PM (UTC-05:00) Eastern Time (US & Canada)

To: PS Media Relations / Relations médias SP

Subject: question re press release

Hi,

I'm a freelance journalist based in Victoria, BC, and I'd like to interview someone asap (as in, immediately), about the following press

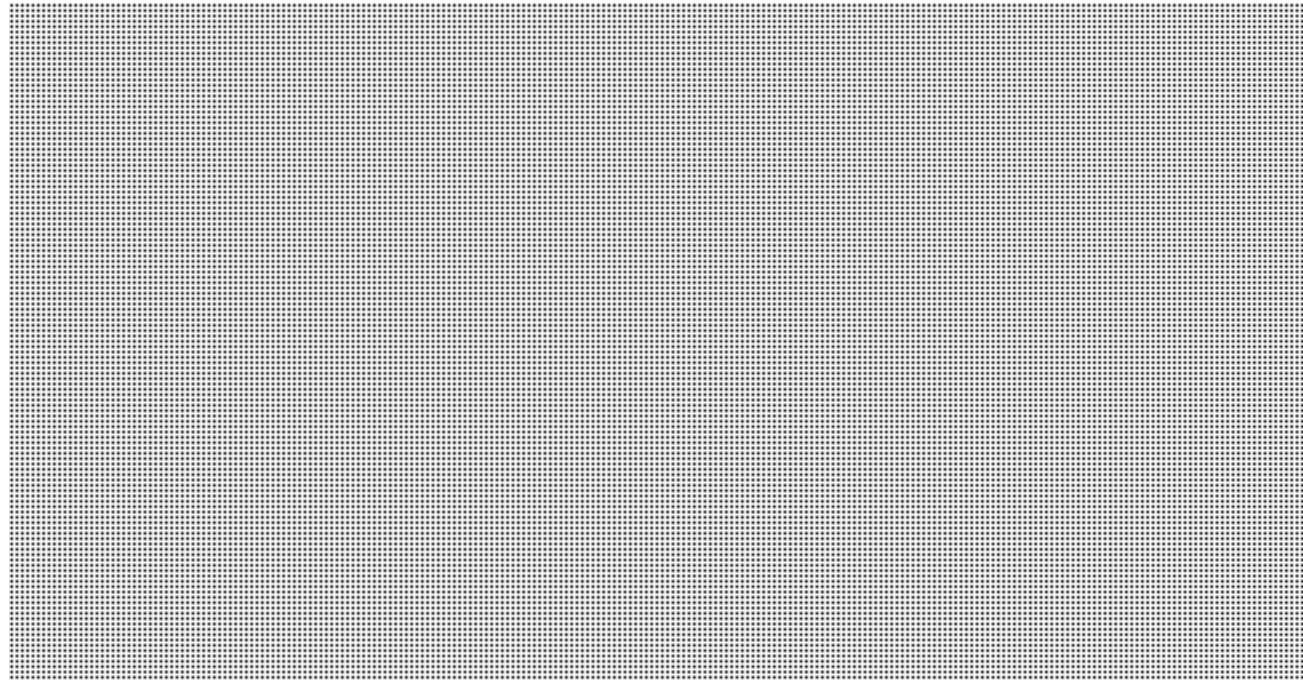
release:

<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.

I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.

thank you,



s.19(1)

Slack, Jessica

From: Patton, Michael
Sent: December-28-11 10:30 AM
To: Slack, Jessica; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'
Cc: Swift, Andrew; Champoux, Martin; Hannan, Andrew; Filipps, Lisa
Subject: Re: Notification: Freelance request on CCIRC Information Note

Approved

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 10:18 AM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca' <nicolas.fortier@pco-bcp.gc.ca>
Cc: Swift, Andrew; Champoux, Martin; Hannan, Andrew; Filipps, Lisa
Subject: RE: Notification: Freelance request on CCIRC Information Note

Revised for approval:

- The subject of CCIRC's notice is known as the cURL library. In computer programming, a library is pre-written code that a software programmer can use instead of writing all code from scratch.
- The cURL library is a popular, open source software tool used to establish an internet connection between two computers, including secure connections. If not implemented properly, there is a risk that secure data could be exposed to interception.
- With this notice, CCIRC is ensuring that information about the risks presented by improper implementation are widely known. These steps include providing public notification on the Public Safety Canada website, and targeted notifications to known users so that they may assess whether they are at risk.

From: Patton, Michael
Sent: Wednesday, December 28, 2011 10:14 AM
To: Slack, Jessica; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'
Cc: Swift, Andrew; Champoux, Martin; Hannan, Andrew; Filipps, Lisa
Subject: Re: Notification: Freelance request on CCIRC Information Note

Thanks Jessica

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 10:06 AM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca' <nicolas.fortier@pco-bcp.gc.ca>
Cc: Swift, Andrew; Champoux, Martin; Hannan, Andrew; Filipps, Lisa
Subject: RE: Notification: Freelance request on CCIRC Information Note

We will try to simplify...

Jessica

From: Patton, Michael
Sent: Wednesday, December 28, 2011 9:55 AM
To: Slack, Jessica; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'

Cc: Swift, Andrew; Champoux, Martin; Hannan, Andrew; Philipps, Lisa
Subject: Re: Notification: Freelance request on CCIRC Information Note

Really do not understand the answer

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 09:38 AM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca' <nicolas.fortier@pco-bcp.gc.ca>
Cc: Swift, Andrew; Champoux, Martin; Hannan, Andrew; Philipps, Lisa
Subject: RE: Notification: Freelance request on CCIRC Information Note

Mike,

Further to this call, here is the proposed response for your approval:

- The subject of CCIRC's notice is known as the cURL library. In computer programming, a library is a pre-written module that can be inserted into a software application to deliver a specific function or action. A software programmer will draw on numerous existing libraries in developing an application rather than always inventing all functionality from scratch.
- The cURL library is a very popular and open source software tool used to establish an internet connection between two computers, including secure connections. If not implemented properly, there is a risk that secure data could be exposed to interception.
- While it is not possible to identify all those who use this library, CCIRC has taken steps to ensure that information about the risks presented by improper implementation are widely known. These steps include providing public notification on the Public Safety Canada website, and targeted notifications to known users so that they may assess whether they are at risk.

From: Slack, Jessica
Sent: Friday, December 23, 2011 1:04 PM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'
Cc: Durand, Stéphanie; Swift, Andrew; Champoux, Martin
Subject: Notification: Freelance request on CCIRC Information Note

Good afternoon,

We've received the following request for an interview on this information note:
<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>
Communications is working with Cyber Security policy on a written response for the reporter which will follow for approval later this afternoon.

Jessica

s.19(1)

Reporter's Name



Media Outlet

Freelance

Call Date 12/23/2011 1:00 PM

Telephone

s.19(1)

E-mail address

Deadline

12/23/2011 5:00 PM

Status

Consulting

Branch

NS

Subject

CCIRC Information Note

Questions

I'm a freelance journalist based in Victoria, BC, and I'd like to interview someone asap (as in, immediately), about the following:

<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.

I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.

Jessica Slack

Media Relations / Relations avec les médias
Public Safety Canada / Sécurité publique Canada
613-949-4288

Slack, Jessica

From: Slack, Jessica on behalf of PS Media Relations / Relations médias SP
Sent: December-28-11 1:01 PM
To: [REDACTED] s.19(1)
Subject: RE: question re press release

Hi again,

We'll do our best to provide you with some answers to your questions, but it will be challenging to do so today as a number of people are on holidays.

Jessica

s.19(1)

-----Original Message-----

From: [REDACTED]
Sent: Wednesday, December 28, 2011 12:26 PM
To: PS Media Relations / Relations médias SP
Subject: Re: question re press release

Thanks, Jessica, but unfortunately it's not useful at all, because this response is as vague as the press release.

Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media?

Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications?

And can you please clarify how the notification list was developed?

Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public?

Can you please explain why there has been no effort to notify news media?

Thank you,

[REDACTED]

s.19(1)

s.19(1)

On 28/12/2011 7:33 AM, PS Media Relations / Relations médias SP wrote:

> Hi [REDACTED]
>
> I have looked into this and hope the following information will be helpful for your article:
>
> The subject of CCIRC's notice is known as the cURL library. In computer programming, a library is pre-written code that a software programmer can use instead of writing all code from scratch.
>
> The cURL library is a popular, open source software tool used to establish an internet connection between two computers, including secure connections. If not implemented properly, there is a risk that secure data could be exposed to interception.
>
> With this notice, CCIRC is ensuring that information about the risks presented by improper implementation are widely known. These steps include providing public notification on the Public Safety Canada website, and targeted notifications to known users so that they may assess whether they are at risk.

> Regards,
> Jessica

> -----Original Message-----

s.19(1)

> From: [REDACTED]
> Sent: Thursday, December 22, 2011 4:34 PM
> To: PS Media Relations / Relations médias SP
> Subject: question re press release

> Hi,
>
> I'm a freelance journalist based in Victoria, BC, and I'd like to
> interview someone asap (as in, immediately), about the following press
> release:
> <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

> I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.

> I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.

> thank you,

s.19(1)

Slack, Jessica

From: Slack, Jessica
Sent: December-28-11 1:31 PM
To: Dick, Robert
Cc: Filipps, Lisa
Subject: FW: question re press release

Hi Robert,

We are thinking that something like the following might work as a response. Can you have a look please and edit as appropriate?

If you could back to us on this by the end of the day, that would be very much appreciated.

Thanks again,
Jessica

PROPOSED RESPONSE FOR INPUT/CONSIDERATION The Canadian Cyber Incident Response Centre issues notifications to individuals and organizations to advise them of risks and mitigation advice related to cyber threats. Its focus is the protection of national critical infrastructure against cyber incidents. The December 20th posting was not a press release, but rather a notification to stakeholders, including critical infrastructure partners such as financial institutions and others.

These notifications are issued on a regular basis and can be found at <http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx> CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analysis, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

As indicated in our earlier response, this information would be of interest to individuals or organizations who have used the cURL library.

Public Safety Canada does not provide spokespeople to speak with media on routine notifications.

The Government of Canada is committed to helping Canadians stay safe online. That is why in October, Public Safety Canada launched getcybersafe.ca, a web site that provides information on how Canadians can protect themselves from a variety of cyber threats.

-----Original Message-----

From: Filipps, Lisa
Sent: Wednesday, December 28, 2011 12:32 PM
To: Dick, Robert
Cc: Slack, Jessica; Hannan, Andrew
Subject: FW: question re press release

Hi Robert - our reporter has come back with a number of questions (see below).

I think we would want to advise that this is not a press release, rather it is a notification that is a regular part of Public Safety's notification process related to its cyber security mandate.

With regards to an interview, we could advise him that we do not make a spokesperson available for operational notifications such as these.

As for the remaining questions, would it be possible to provide some background on how the notification list is created? Is this particular issue of concern to the general public?

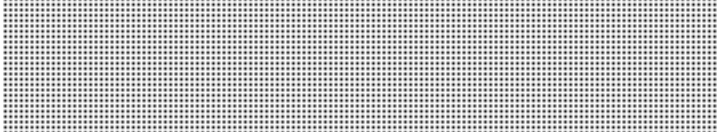
Please feel free to call me if you wish to discuss approach.

Lisa
949-9741

-----Original Message-----

From: PS Media Relations / Relations médias SP
Sent: Wednesday, December 28, 2011 12:26 PM
To: Swift, Andrew; Fergusson, Janis; Filippis, Lisa; McDonald, Jessica
Subject: FW: question re press release

s.19(1)

From: 
Sent: Wednesday, December 28, 2011 12:27:46 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: Re: question re press release

Thanks, Jessica, but unfortunately it's not useful at all, because this response is as vague as the press release.

Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media?

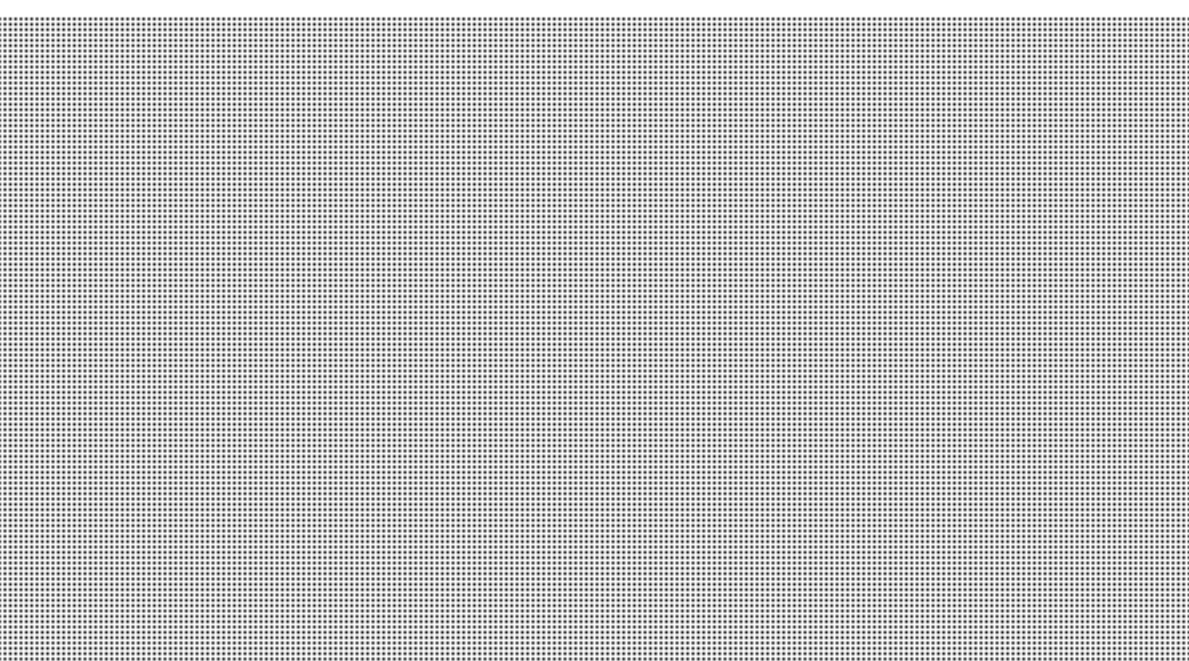
Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications?

And can you please clarify how the notification list was developed?

Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public?

Can you please explain why there has been no effort to notify news media?

Thank you,



s.19(1)

s.19(1)

On 28/12/2011 7:33 AM, PS Media Relations / Relations médias SP wrote:

> Hi [REDACTED]
>
> I have looked into this and hope the following information will be helpful for your article:
>
> The subject of CCIRC's notice is known as the cURL library. In computer programming, a library is pre-written code that a software programmer can use instead of writing all code from scratch.
>
> The cURL library is a popular, open source software tool used to establish an internet connection between two computers, including secure connections. If not implemented properly, there is a risk that secure data could be exposed to interception.
>
> With this notice, CCIRC is ensuring that information about the risks presented by improper implementation are widely known. These steps include providing public notification on the Public Safety Canada website, and targeted notifications to known users so that they may assess whether they are at risk.

> Regards,
> Jessica

> -----Original Message-----

> From: [REDACTED]
> Sent: Thursday, December 22, 2011 4:34 PM
> To: PS Media Relations / Relations médias SP
> Subject: question re press release

s.19(1)

>
> Hi,
>
> I'm a freelance journalist based in Victoria, BC, and I'd like to
> interview someone asap (as in, immediately), about the following press
> release:
> <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>
>
> I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.
>
> I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.
>
> thank you,

[REDACTED]

s.19(1)

>
>
>

Media Enquiries - Rob Wipond

Fiscal Year	2011/2012	s.19(1)
Reporter's Name		
Media Outlet	Freelance	
Call Date	12/28/2011 2:00 PM	
Telephone		
E-mail address		
Deadline		
Status	Final	
Branch	NS	
Subject	CCIRC notice	
Questions	Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media? Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications? And can you please clarify how the notification list was developed? Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public? Can you please explain why there has been no effort to notify news media?	
Reporter and Outlet		Freelance
Actions Taken	No existing entries.	s.19(1)
Draft Response		
Approvals	Robert Dick (verbally to Lisa and I) Andrew H, Mike	
Final Response	Please note that the December 20th posting was not a press release, but rather a routine notification to stakeholders, including critical infrastructure partners such as financial institutions and others. Public Safety Canada does not provide spokespeople to speak with media on routine notifications such as this. As indicated in our earlier response, this information would be of interest to individuals or organizations who have used the cURL library. The Canadian Cyber Incident Response Centre issues notifications to individuals and organizations to advise them of risks and mitigation advice related to cyber threats. Its focus is the protection of national critical infrastructure against cyber incidents. CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. As a service to IT professionals and managers of critical infrastructure and other related industries, the Centre provides analysis, as well as a variety of information products. Ultimately, private companies are responsible for being aware of cyber threats and ensuring the integrity of their systems. It would not be appropriate for the department to disclose a list of companies that have received direct notifications.	
Notes		
Media Coverage		

Slack, Jessica

From: Slack, Jessica
Sent: December-28-11 2:30 PM
To: Filipps, Lisa
Subject: FW: question re press release

Public Safety Canada does not provide spokespeople to speak with media on routine notifications such as this. As indicated in our earlier response, this information would be of interest to individuals or organizations who have used the cURL library.

The Canadian Cyber Incident Response Centre issues notifications to individuals and organizations to advise them of risks and mitigation advice related to cyber threats. Its focus is the protection of national critical infrastructure against cyber incidents. The December 20th posting was not a press release, but rather a notification to stakeholders, including critical infrastructure partners such as financial institutions and others.

CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. The Centre provides analysis, as well as a variety of information products and services specifically for IT professionals and managers of critical infrastructure and other related industries.

Ultimately, private companies are responsible for the integrity of their systems.

-----Original Message-----

From: Filipps, Lisa
Sent: Wednesday, December 28, 2011 12:32 PM
To: Dick, Robert
Cc: Slack, Jessica; Hannan, Andrew
Subject: FW: question re press release

Hi Robert - our reporter has come back with a number of questions (see below).

I think we would want to advise that this is not a press release, rather it is a notification that is a regular part of Public Safety's notification process related to its cyber security mandate.

With regards to an interview, we could advise him that we do not make a spokesperson available for operational notifications such as these.

As for the remaining questions, would it be possible to provide some background on how the notification list is created? Is this particular issue of concern to the general public?

Please feel free to call me if you wish to discuss approach.

Lisa
949-9741

-----Original Message-----

From: PS Media Relations / Relations médias SP
Sent: Wednesday, December 28, 2011 12:26 PM
To: Swift, Andrew; Fergusson, Janis; Filippis, Lisa; McDonald, Jessica
Subject: FW: question re press release

s.19(1)

From: [REDACTED]
Sent: Wednesday, December 28, 2011 12:27:46 PM (UTC-05:00) Eastern Time (US & Canada)
To: PS Media Relations / Relations médias SP
Subject: Re: question re press release

Thanks, Jessica, but unfortunately it's not useful at all, because this response is as vague as the press release.

Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media?

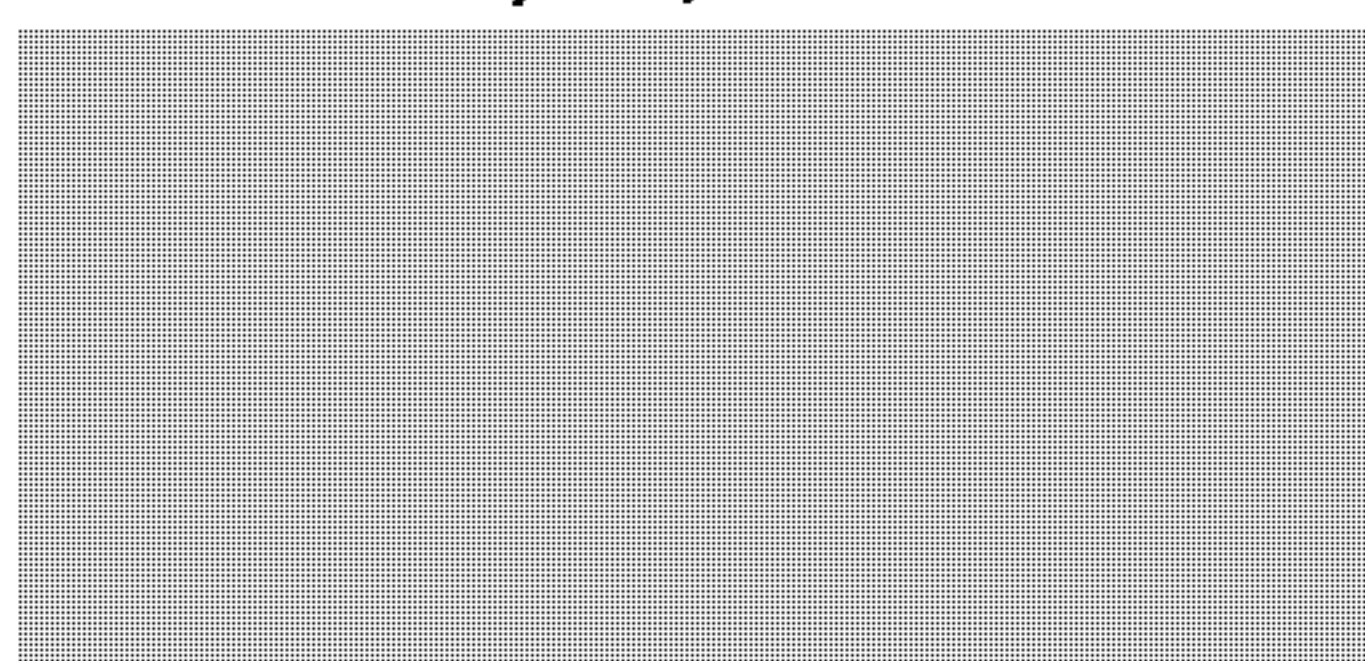
Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications?

And can you please clarify how the notification list was developed?

Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public?

Can you please explain why there has been no effort to notify news media?

Thank you,



s.19(1)

On 28/12/2011 7:33 AM, PS Media Relations / Relations médias SP wrote: s.19(1)

> Hi [REDACTED]
>

> I have looked into this and hope the following information will be helpful for your article:

>
> The subject of CCIRC's notice is known as the cURL library. In computer programming, a library is pre-written code that a software programmer can use instead of writing all code from scratch.
>
> The cURL library is a popular, open source software tool used to establish an internet connection between two computers, including secure connections. If not implemented properly, there is a risk that secure data could be exposed to interception.
>
> With this notice, CCIRC is ensuring that information about the risks presented by improper implementation are widely known. These steps include providing public notification on the Public Safety Canada website, and targeted notifications to known users so that they may assess whether they are at risk.

>
> Regards,
> Jessica

s.19(1)

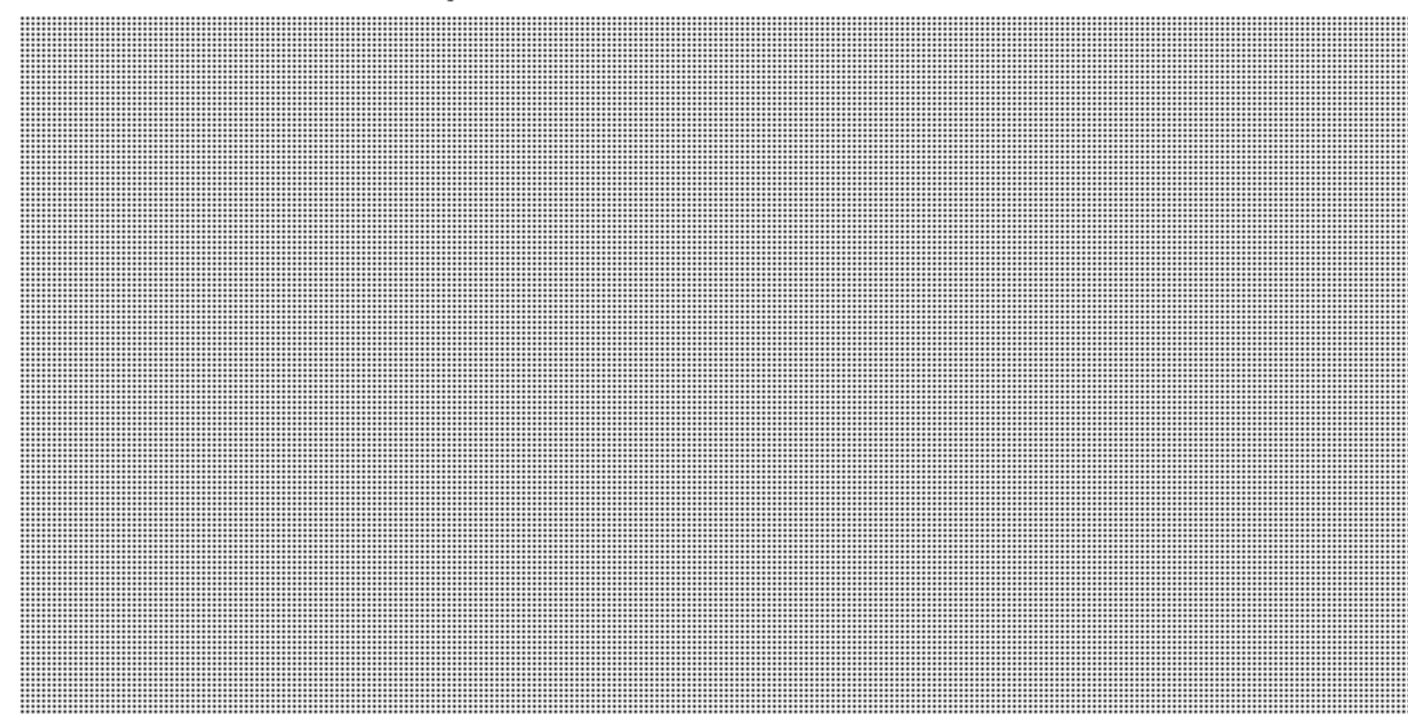
> -----Original Message-----

> From: 
> Sent: Thursday, December 22, 2011 4:34 PM
> To: PS Media Relations / Relations médias SP
> Subject: question re press release

>
> Hi,
>
> I'm a freelance journalist based in Victoria, BC, and I'd like to
> interview someone asap (as in, immediately), about the following press
> release:
> <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>
>
> I would like someone who can explain in more 'layperson's terms' what this vulnerability is, how important it is, what it affects, who it affects etc.

>
> I'm on pacific time, so if the call is coming not today but Friday morning, then after 11 a.m. eastern time is acceptable.
>
> thank you,

s.19(1)



>
>

Slack, Jessica

From: Slack, Jessica
Sent: December-29-11 9:06 AM
To: Hannan, Andrew
Cc: Filipps, Lisa
Subject: RE: Notification: Follow-up questions on CCIRC Notice

Andrew...just following up. Let us know if you have any questions.
Jessica

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 2:54 PM
To: Hannan, Andrew; Bue, Richard; Salewski, Shawn
Cc: Filipps, Lisa
Subject: FW: Notification: Follow-up questions on CCIRC Notice

Andrew,

Proposed response to the reporter's follow-ups. Robert Dick came by and we discussed the response with him.

Jessica

The December 20th posting was not a press release, but rather a routine notification to stakeholders, including critical infrastructure partners such as financial institutions and others. Public Safety Canada does not provide spokespeople to speak with media on routine notifications such as this.

As indicated in our earlier response, this information would be of interest to individuals or organizations who have used the cURL library.

The Canadian Cyber Incident Response Centre issues notifications to individuals and organizations to advise them of risks and mitigation advice related to cyber threats. Its focus is the protection of national critical infrastructure against cyber incidents.

CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. As a service to IT professionals and managers of critical infrastructure and other related industries, the Centre provides analysis, as well as a variety of information products.

Ultimately, private companies are responsible for being aware of cyber threats and ensuring the integrity of their systems.

It would not be appropriate for the department to disclose a list of companies that have received direct notifications.

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 1:22 PM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'
Cc: Hannan, Andrew; Filipps, Lisa
Subject: Notification: Follow-up questions on CCIRC Notice

Good afternoon,

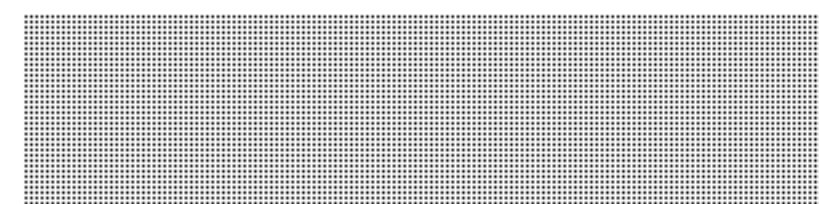
We have received follow-up questions regarding the CCIRC notice:

Action: Comms consulting with Cyber Security policy.

Jessica

s.19(1)

Reporter's Name



Media Outlet

Freelance

Call Date

12/28/2011 2:00 PM

Telephone

E-mail address

Deadline

Status

Consulting

Branch

NS

Subject

CCIRC notice

Questions

Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media?

Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications?

And can you please clarify how the notification list was developed?

Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public?

Can you please explain why there has been no effort to notify news media?

Slack, Jessica

From: Slack, Jessica
Sent: December-29-11 9:09 AM
To: Patton, Michael; 'nfortier@pco-bcp.gc.ca' (nfortier@pco-bcp.gc.ca); Carmichael, Julie
Cc: Filipps, Lisa; Hannan, Andrew
Subject: FOR APPROVAL: Follow-up questions on CCIRC Notice

Mike,

Proposed response to the reporter's follow-up questions for your approval, please.

Many thanks,
Jessica

PROPOSED RESPONSE

The December 20th posting was not a press release, but rather a routine notification to stakeholders, including critical infrastructure partners such as financial institutions and others. Public Safety Canada does not provide spokespeople to speak with media on routine notifications such as this.

As indicated in our earlier response, this information would be of interest to individuals or organizations who have used the cURL library.

The Canadian Cyber Incident Response Centre issues notifications to individuals and organizations to advise them of risks and mitigation advice related to cyber threats. Its focus is the protection of national critical infrastructure against cyber incidents.

CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. As a service to IT professionals and managers of critical infrastructure and other related industries, the Centre provides analysis, as well as a variety of information products.

Ultimately, private companies are responsible for being aware of cyber threats and ensuring the integrity of their systems.

It would not be appropriate for the department to disclose a list of companies that have received direct notifications.

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 1:22 PM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'
Cc: Hannan, Andrew; Filipps, Lisa
Subject: Notification: Follow-up questions on CCIRC Notice

Good afternoon,

We have received follow-up questions regarding the CCIRC notice:

Action: Comms consulting with Cyber Security policy.
Jessica

s.19(1)

Reporter's Name



Media Outlet

Freelance

Call Date

12/28/2011 2:00 PM

Telephone

E-mail address

Deadline

Status

Consulting

Branch

NS

Subject

CCIRC notice

Questions

Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media?

Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications?

And can you please clarify how the notification list was developed?

Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public?

Can you please explain why there has been no effort to notify news media?

Slack, Jessica

From: Slack, Jessica
Sent: December-29-11 9:12 AM
To: Dick, Robert
Cc: Filipps, Lisa
Subject: FYI Follow-up questions on CCIRC Notice

Hi Robert...just fyi. Here is the response that MO just approved.

Thanks for your help yesterday.
Jessica

PROPOSED RESPONSE

The December 20th posting was not a press release, but rather a routine notification to stakeholders, including critical infrastructure partners such as financial institutions and others. Public Safety Canada does not provide spokespeople to speak with media on routine notifications such as this.

As indicated in our earlier response, this information would be of interest to individuals or organizations who have used the cURL library.

The Canadian Cyber Incident Response Centre issues notifications to individuals and organizations to advise them of risks and mitigation advice related to cyber threats. Its focus is the protection of national critical infrastructure against cyber incidents.

CCIRC works with national and international counterparts to collect, analyze and disseminate data on cyber threats. As a service to IT professionals and managers of critical infrastructure and other related industries, the Centre provides analysis, as well as a variety of information products.

Ultimately, private companies are responsible for being aware of cyber threats and ensuring the integrity of their systems.

It would not be appropriate for the department to disclose a list of companies that have received direct notifications.

From: Slack, Jessica
Sent: Wednesday, December 28, 2011 1:22 PM
To: Patton, Michael; Carmichael, Julie; Johnson, Mark; 'nicolas.fortier@pco-bcp.gc.ca'
Cc: Hannan, Andrew; Filipps, Lisa
Subject: Notification: Follow-up questions on CCIRC Notice

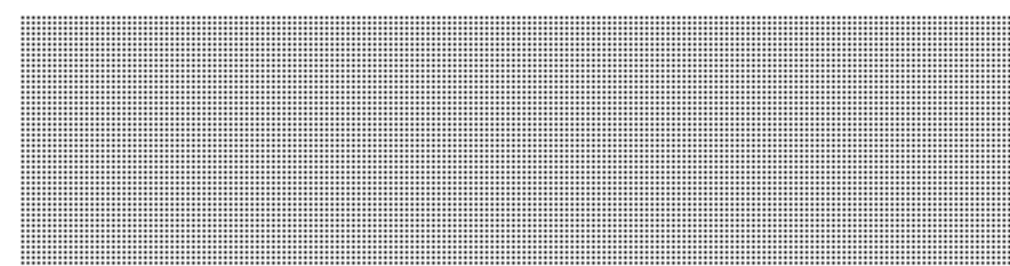
Good afternoon,

We have received follow-up questions regarding the CCIRC notice:

Action: Comms consulting with Cyber Security policy.
Jessica

s.19(1)

Reporter's Name



Media Outlet	Freelance
Call Date	12/28/2011 2:00 PM
Telephone	
E-mail address	
Deadline	
Status	Consulting
Branch	NS
Subject	CCIRC notice
Questions	Can you please explain why there is no knowledgeable person available to provide an interview? When will a person be made available? Is it normal procedure for Public Safety Canada and CCIRC to issue a press release for which no one is made available to speak to news media? Could you please send me the list of companies that have received direct notifications from Public Safety Canada and CCIRC? Failing that, could you please send me a list of the types of companies that have been sent direct notifications, and an approximate number for how many companies have been sent notifications? And can you please clarify how the notification list was developed? Can you please provide an explanation for how urgent or concerning this issue is or should be for e-commerce providers and the general public? Can you please explain why there has been no effort to notify news media?

s.16(2)(c)

s.20(1)(c)

DRAFT FOR COMMENTS AND REVIEW

La version française suit

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-XXX
Date:

IMPLEMENTATING PHP CURL VERIFYPEER OPTION IN APPLICATIONS REQUIRING SSL CERTIFICATE
VERIFICATION

PURPOSE
=====

The goal of this advisory is to raise awareness of a common but potentially insecure
implementation of the PHP CURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It
allows developers to dynamically generate HTML pages. PHP implements a number of
standard code libraries including Client URL (cURL or libcurl). The cURL library
provides a set of functions which allow establishing connections using various
communication protocols including HTTPS. This library is also responsible for
implementing security features such as the validation of SSL certificates when
establishing HTTPS connections. The cURL library is commonly used by web application
developers, particularly in electronic commerce applications, to establish secure
connections between systems hosted on different network segments, such as
connections to third-party payment card processing services.

Within the PHP CURL library, the curl_setopt function allows for the setting of a
number of run-time options, including the configuration of how SSL certificates will
be verified against relevant Certificate Authorities. The option
CURLOPT_SSL_VERIFYPEER defines whether the library will attempt trust validation of
SSL certificates when establishing secure connections. When enabled cURL will
attempt to verify the remote server's certificate against one or more trusted
Certificate Authorities as defined by either of the configuration options
CURLOPT_CAINFO or CURLOPT_CAPATH. The CURLOPT_SSL_VERIFYPEER option is enabled by
default and on certain platforms a list of Certificate Authorities is predefined.
Unfortunately, this validation framework is often disabled entirely by developers
setting the CURLOPT_SSL_VERIFYPEER option to "0", or "false". When peer verification
is disabled, SSL certificates are not trust-validated by cURL. Failure of the
application to properly validate SSL certificates provides opportunity for a number
of man-in-the-middle attack scenarios potentially leading to interception and
modification of data in transit.

The cURL functions are generally used for server-to-server communications and as a
result application operators, such as merchants in electronic commerce, may not be
aware that their applications are transacting using potentially unsecured
communications channels.

..
..
..
..
..
..
..
..
..
..
..
..

SUGGESTED ACTION

=====

CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP CURL library, verify that the CURLOPT_SSL_VERIFYPEER option is not set to boolean value false, or integer value 0, and that failure to return a successful verification results in a failed connection error rather than establishment of an untrusted and unsecured connection. Searching application source code directory for the entries similar to the following will provide indications of the settings used in your CURL implementation:

Examples:

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 1);
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 0);
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, true);
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");
curl_setopt($connection, CURLOPT_CAPATH, "path:/");
```

Specifically the strings "CURLOPT_SSL_VERIFYPEER", "CURLOPT_CAINFO" and "CURLOPT_CAPATH" should be searched.

CCIRC recommends that transaction processing organisations review and ensure that their distributed PHP APIs enforce proper implementation of certificate verification by affiliated merchants and partners accordingly.

Where possible, it is recommended that developers of secure applications pin certificate validation against the specific CA certificate that will be used. This can be achieved using the CURLOPT_CAINFO option and distributing the associated public CA certificate alongside program code in the same software package.

CCIRC recommends that operators of web applications regularly verify availability of updates and patches for their software packages, as well as test and deploy these in a timely manner, accordingly.

CREDIT

=====

CCIRC would like to thank Kevin McArthur from StormTide Digital Studios Inc and Tamir Israel from CIPPIC for their research and contribution to this product.

s.16(2)(c)

s.20(1)(c)

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

SÉCURITÉ PUBLIQUE ET PROTECTION CIVILE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

NOTE D'INFORMATION

Numéro : IN11-XXX
Date :

OBJET
=====

ÉVALUATION
=====

Produits touchés :

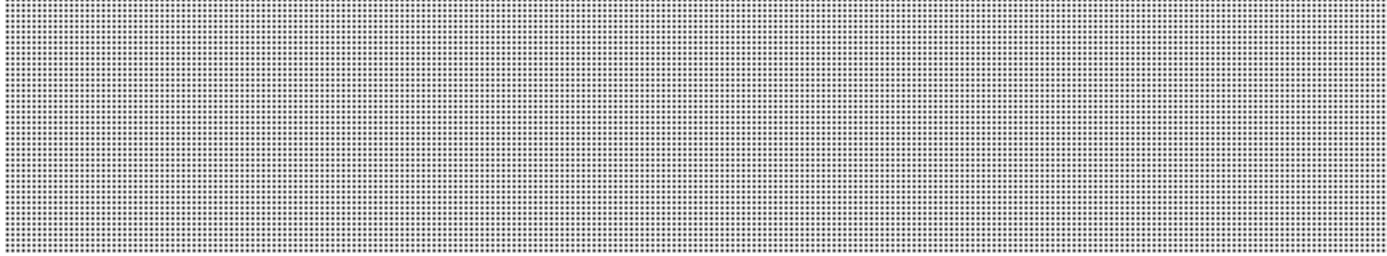
-

ACTION SUGGÉRÉE
=====

Références :

s.16(2)(c)

s.20(1)(c)



Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118

Télécopieur : 613-998-9589

Courriel : communications@ps-sp.gc.ca

Breault, Stephen

From: [REDACTED]
Sent: Monday, July 18, 2011 2:13 PM
To: Beaudoin, Luc S
Subject: FW: Security Vulnerability In [REDACTED]
Attachments: [REDACTED]

Follow Up Flag: Follow up
Flag Status: Completed

This looks like a vulnerability in [REDACTED] credit card type devices. Patch has been issued.

Thoughts on what to do next?

Julia Scouten CISSP GCIA GCIH GSEC

Incident Handler

Canadian Cyber Incident Response Centre (CCIRC) Public Safety Canada Julia.Scouten@ps-sp.gc.ca

613-991-7070

-----Original Message-----

From: [REDACTED]
Sent: July 15, 2011 1:34 PM
To: [REDACTED]
Subject: FW: Security Vulnerability In [REDACTED]

FYA, acknowledge receipt.

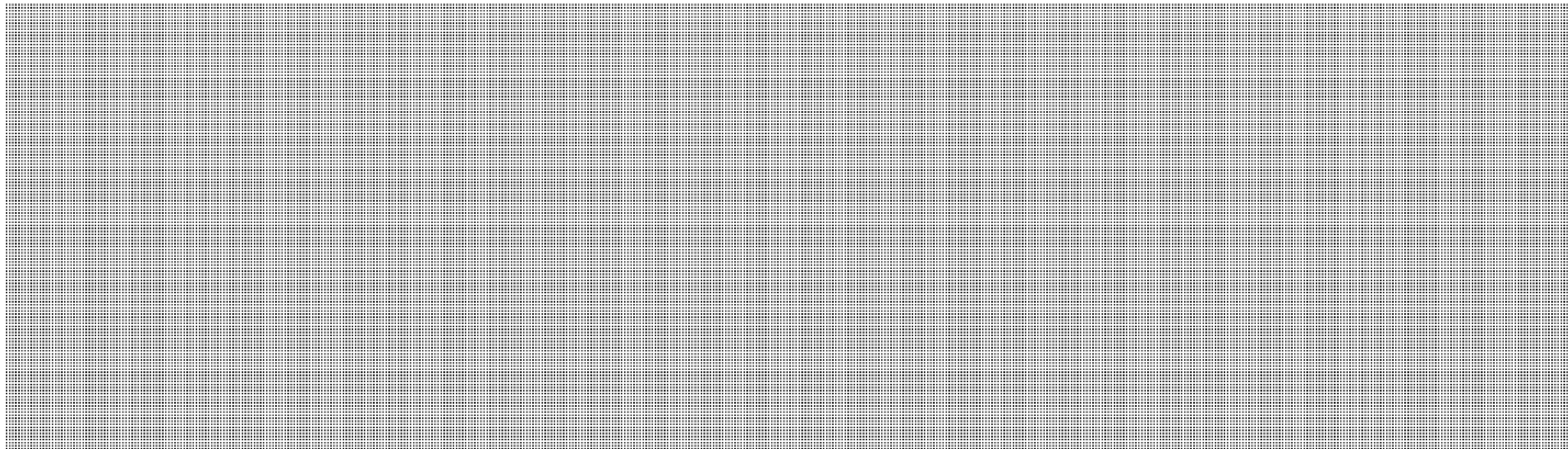
Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: July 15, 2011 1:28 PM
To: [REDACTED] notification@priv.gc.ca
Cc: [REDACTED]
Subject: Security Vulnerability In [REDACTED]

[REDACTED]

--



s.19(1)

s.20(1)(c)

s.16(1)(b)

s.16(2)(c)

s.19(1)

s.28(1)(c)

Breault, Stephen

From: Beaudoin, Luc S
Sent: Monday, July 18, 2011 3:55 PM
To: [REDACTED]
Subject: U2 - N1 Vulnerability in Moneris
Attachments: [REDACTED]

Follow Up Flag: Follow up
Flag Status: Completed

*** PGP SIGNATURE VERIFICATION ***

*** Status: Good Signature

*** Signer: Luc Beaudoin <luc.beaudoin@ps-sp.gc.ca> (0x9FE834DA)

*** Signed: 18/07/2011 3:55:01 PM

*** Verified: 18/07/2011 4:29:14 PM

*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***

U2 - N1

Gents, I would like the [REDACTED] to be aware of this and provide comments/assessments to me.

I have contacted [REDACTED] and have confirmed that an update was posted on their website for their clients.

If you have specific questions you would like us to proxy back to the researcher or the vendor, please let me know.

Regards.

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

*** END PGP DECRYPTED/VERIFIED MESSAGE ***

Security Vulnerability

Thursday July 14, 2011 (Updated: July 15, 2011)

Author:

Affected Versions: 2.03 (php)

Description:

is an interface for the PHP programming language that facilitates the processing of credit cards through the

The API fails to properly validate the SSL trust chain for the connection between the payment gateway and merchant website.

Technical Description:

The PHP CURL extension to send and receive data between the payment processing gateway.

The vulnerability exists in the API's PHP code. Specifically the API code overrides the default libcurl settings and disables SSL Peer Verification:

```
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
```

With this API option set, the SSL certificate trust chain is not validated allowing for a self-signed, untrusted SSL certificate to impersonate

Exploitation Method:

Difficulty: Minimal

- 1) DNS resolution for is overridden. This can occur in many different ways, however, the most common attacks are:
 - a) Changing the /etc/hosts file on a target webserver to overwrite the local DNS value for to an attackers IP address.
 - b) DNS Cache Poisoning (see https://secure.wikimedia.org/wikipedia/en/wiki/DNS_cache_poisoning)
 - c) A malicious actor at the server's DNS provider.
 - d) Other DNS infrastructure attacks. (Eg hacking the A record of the actual domain)
- 2) The attacker must provide a HTTPS enabled web-server and a self-signed SSL certificate containing the CN The attacker may also setup a (Man-In-The-Middle) MITM HTTPS proxy script in order to resubmit requests to the proper gateway and respond correctly with the provided response -- making detection of exploitation extremely difficult.

Note: In certain scenarios DNS control may not be necessary. More sophisticated attacks involving directly intercepting and changing network traffic may also be effective.

Since the [REDACTED] has disabled SSL Peer Verification, the attacker's Self-Signed certificate will be accepted as valid and the merchant's web-server will transmit the credit card information to the attacker and may receive a response from the attacker as if he/she were the [REDACTED] payment gateway.

The merchant or the payment gateway are unlikely to notice a MITM attack performed in this manner as transactions will likely still be submitted and responses returned. Credit card settlements would be unaffected when attacked using a man-in-the-middle methodology, and as such, an attack may go unnoticed indefinitely.

Damage: High

- Allows for the interception of Credit Card and other personal information.
- Allows for Man In The Middle attack on critical infrastructure.
- Exploitation is not easily detected and there is limited evidence of attack once complete.

Resolution [REDACTED]:

- 1) Re-enable SSL Peer Verification.
curl_setopt(\$ch, CURLOPT_SSL_VERIFYPEER, 1);
- 2) Notify customers of vulnerability.
- 3) Reject transaction requests that contain a HTTP User Agent of [REDACTED] or earlier versions to force upgrade to secured version of API.

Resolution (by Merchant)

- 1) Re-enable SSL Peer Verification.
curl_setopt(\$ch, CURLOPT_SSL_VERIFYPEER, 1);

Responsibly submitted in confidence, Thursday July 14 2011.

Intended submission and disclosure timeline:

[REDACTED]
Canadian Cyber Incident Response Centre [REDACTED] [July 15, 2011]
Full Public Disclosure [July 22, 2011, or when vendor publicly acknowledges/releases patch]

Resolution:

July 15: Vendor informs it has patched software and is working towards notifying customers.

s.16(2)(c)

s.19(1)

s.20(1)(c)

Turbide, Frank

From: [REDACTED]
Sent: July-19-11 8:53 AM
To: Turbide, Frank
Subject: FW: Security Vulnerability [REDACTED]
Attachments: [REDACTED]

Julia Scouten CISSP GCIA GCIH GSEC
Incident Handler
Canadian Cyber Incident Response Centre (CCIRC) Public Safety Canada Julia.Scouten@ps-sp.gc.ca
613-991-7070

-----Original Message-----

From: [REDACTED]
Sent: July 15, 2011 1:34 PM
To: [REDACTED]
Subject: FW: Security Vulnerability [REDACTED]

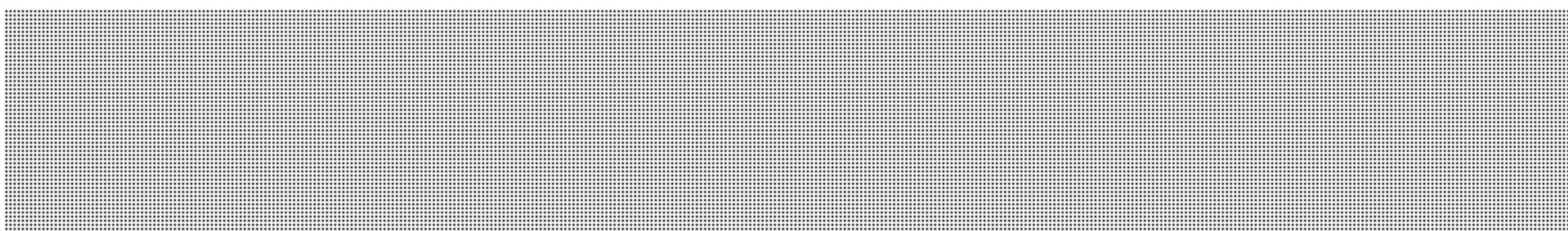
FYA, acknowledge receipt.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: July 15, 2011 1:28 PM
To: [REDACTED] notification@priv.gc.ca
Cc: [REDACTED]
Subject: Security Vulnerability In Moneris [REDACTED]





s.19(1)

s.20(1)(c)

s.16(2)(c)

s.19(1)

s.20(1)(c)

Turbide, Frank

From: Cameron, Bud
Sent: August-29-11 11:16 AM
To: Beaudoin, Luc S; Moore, Bruce
Cc: Turbide, Frank
Subject: FW: Security Vulnerability [REDACTED]
Attachments: [REDACTED]

Importance: High

Just got a call from NCSD, Bob Gordon received something similar from Bill Wilson in the Privacy Commish office. It sounds like an ethical hacker who is frustrated at his attempts at responsible disclosure. NCSD wants somebody to talk to this guy and assure him we are doing something. Before I will do that, need more info and who is doing what to fix this vulnerability, if it is indeed serious.

-----Original Message-----

From: [REDACTED]
Sent: August 29, 2011 11:13 AM
To: Cameron, Bud
Subject: FW: Security Vulnerability In [REDACTED]

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: July 15, 2011 1:34 PM
To: [REDACTED]
Subject: FW: Security Vulnerability [REDACTED]

FYA, acknowledge receipt.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

-----Original Message-----

From: [REDACTED]
Sent: July 15, 2011 1:28 PM
To: [REDACTED] notification@priv.gc.ca
Cc: [REDACTED]
Subject: Security Vulnerability In Moneris [REDACTED]

[REDACTED]

s.16(2)(c)

s.19(1)

s.20(1)(c)



s.16(2)(c)

s.20(1)(c)

Breault, Stephen

From: Cameron, Bud
Sent: Monday, August 29, 2011 11:56 AM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: Activity 2971 [REDACTED] vulnerability

Follow Up Flag: Follow up
Flag Status: Completed

Noted, and from the tone I don't think Craig wants us to talk to the researcher, that's fine. It's NCSD that wants us to talk to researcher.

-----Original Message-----

From: Beaudoin, Luc S
Sent: August 29, 2011 11:32 AM
To: Cameron, Bud
Cc: [REDACTED]
Subject: RE: Activity 2971 [REDACTED] vulnerability

There is an update available from the vendor which apparently addresses the vulnerability. We cannot validate this here but the issue of the researcher is that users of [REDACTED] may not have been informed appropriately to update their product. This is the issue I brought to the legal staff from [REDACTED] who I spoke with, so that they notify their clients. We have not heard back from them but we will follow up accordingly with them.

Note that one needs to be careful prior to engaging with an unknown security researcher so that we have all information at hand and we respect the principles of responsible disclosure with the vendor.

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

-----Original Message-----

From: Cameron, Bud
Sent: August 29, 2011 11:28 AM
To: Beaudoin, Luc S

Cc: [REDACTED]
Subject: RE: Activity 2971 [REDACTED] vulnerability

So according to this note, the code fix has already been issued?

s.16(1)(b)

s.16(2)(c)

s.19(1)

s.20(1)(c)

-----Original Message-----

From: Beaudoin, Luc S
Sent: August 29, 2011 11:26 AM
To: Cameron, Bud
Cc: [REDACTED]
Subject: Activity 2971 [REDACTED] vulnerability

Short Description [REDACTED] vulnerability disclosure tracking

Detail Description [REDACTED]

Phone call 13h, 19 Jul, [REDACTED] is still investigating the claim of the vulnerability.

Received an [REDACTED] GOC. Luc contacted [REDACTED] to validate the content of the email. [REDACTED] confirmed they were contacted last week and have issued a fixed code for the [REDACTED] manager may call Luc back to answer questions wrt informing customers of the vulnerability.

Sent an email to the [REDACTED] to get their feedback and raise their awareness

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

s.20(1)(c)

Breault, Stephen

From: Beaudoin, Luc S
Sent: Monday, August 29, 2011 4:15 PM
To: [REDACTED] Cameron, Bud
Subject: RE: Activity 2971 [REDACTED] vulnerability

Follow Up Flag: Follow up
Flag Status: Completed

I called [REDACTED] again and I insisted on the vulnerability disclosure process, whereby a vulnerability needs to be publicized if we want people to patch it. Now I suggested that the better way to do this is to reach clients directly, so that not everyone else knows about the exposure. I also mentioned that a vulnerability may be addressed at an other level of the infrastructure, such as adding an encryption wrapper, or a detection mechanism on the server side for man-in-the-middle attacks. The contact [REDACTED] is just coming back from leave and will get update tomorrow and get back to us.

One question was whether this information from the Privacy Commiss. is new or if it is the same information reported back in July. The reason is [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

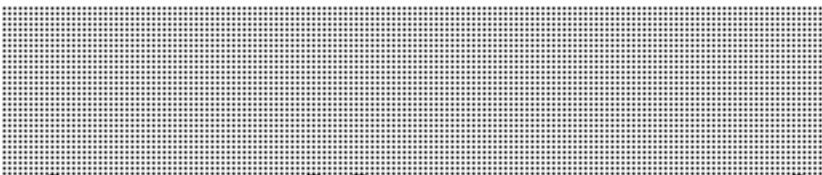
-----Original Message-----

From: [REDACTED]
Sent: August 29, 2011 3:29 PM
To: Cameron, Bud; Beaudoin, Luc S; CYBERDO
Subject: RE: Activity 2971 [REDACTED] vulnerability

[REDACTED] would not comment one way or the other if their clients were notified, so I couldn't speculate.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC

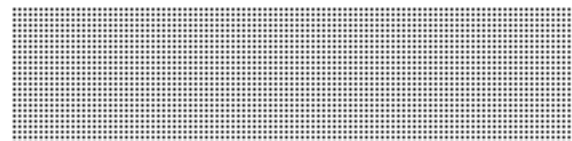
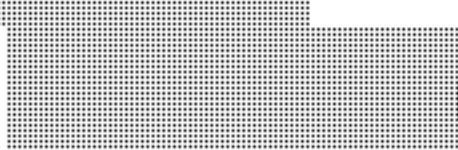
s.16(2)(c)

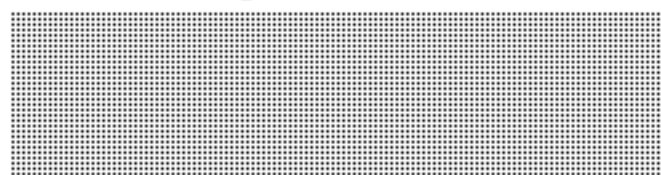

<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

s.21(1)(a)

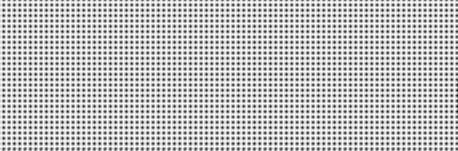
s.20(1)(c)

-----Original Message-----

From: Cameron, Bud
Sent: August 29, 2011 3:10 PM
To: Beaudoin, Luc S; 
Subject: RE: Activity 2971  vulnerability

So you don't believe the clients were notified, or is this software resold or embedded such that any notification of clients  would be incomplete?

-----Original Message-----

From: Beaudoin, Luc S
Sent: August 29, 2011 2:36 PM
To: Cameron, Bud; 
Subject: Re: Activity 2971  vulnerability

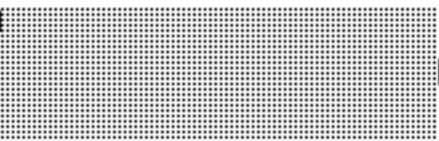
I think this could be a good case where we need to work with  to assess the impact and risk further and if it falls into a level of significance high enough to distribute a product, so be it...this would be our first advisory of non-NVD stuff...

Luc Beaudoin

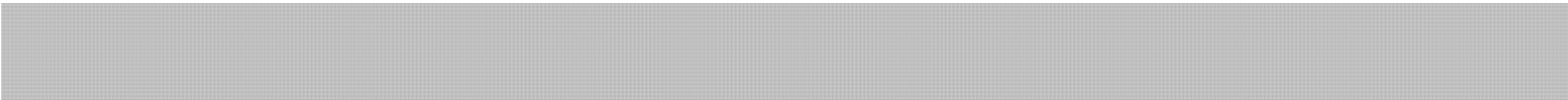
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----

From: Cameron, Bud
To: Oldham, Craig
Cc: Beaudoin, Luc S
Sent: Mon Aug 29 14:24:21 2011
Subject: FW: Activity 2971  vulnerability

See Bruce's note below. One further note - in July Luc had offered to assist in notifying clients, via a CCIRC product, and  declined.


Bud

-----Original Message-----

From: 
Sent: August 29, 2011 2:18 PM
To: Cameron, Bud
Cc:  Beaudoin, Luc S
Subject: RE: Activity 2971  vulnerability

s.16(2)(c)

s.20(1)(c)

Response from a representative of [REDACTED]

The vulnerability has been fixed and updated software is available.

The representative would not comment on how their clients were notified. This was handled internally and they feel the matter was addressed. There is no government regulation requiring [REDACTED] inform (CCIRC or the government) on these types of issues and they would not comment further.

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[REDACTED]

<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

-----Original Message-----

From: Cameron, Bud
Sent: August 29, 2011 2:08 PM
To: Moore, Bruce
Cc: [REDACTED] Beaudoin, Luc S
Subject: RE: Activity 2971 [REDACTED] vulnerability

Yes please.

-----Original Message-----

From: Moore, Bruce
Sent: August 29, 2011 2:07 PM
To: Cameron, Bud
Cc: [REDACTED] Beaudoin, Luc S
Subject: RE: Activity 2971 [REDACTED] vulnerability

I'm assuming you mean the Vendor [REDACTED] - To ask if they have notified their clients.

I'll call the [REDACTED] POC listed under the activity and see what they have to say (assuming I get a hold of them or get a response today).

Bruce Moore
Cyber Duty Officer
Public Safety Canada
CCIRC
[REDACTED]

<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

-----Original Message-----

From: Cameron, Bud
Sent: August 29, 2011 1:57 PM

s.16(2)(c)

To: Moore, Bruce
Subject: FW: Activity 2971 [REDACTED] vulnerability

s.19(1)

s.21(1)(a)

s.20(1)(c)

Bruce can you call these guys and get the basic facts Craig is demanding?

-----Original Message-----

From: Oldham, Craig
Sent: August 29, 2011 1:56 PM
To: Cameron, Bud
Subject: RE: Activity 2971 [REDACTED] vulnerability

Think someone needs to talk directly to the vendor and sort this out?

In the end all I want to say to the researcher is: The problem was identified, a fix was put in place, the vendor's clients were told. No other details - but we need to be sure this is accurate.

S. Craig Oldham

A/Director General Operations - Directeur général aux opérations intérimaire Government Operations Centre – Centre des opérations du gouvernement Office (613) 991-7728 Secure (613) 996-1088
Cell (613) 299-2114 Craig.Oldham@ps.gc.ca

-----Original Message-----

From: Oldham, Craig
Sent: August 29, 2011 1:49 PM
To: Cameron, Bud
Subject: RE: Activity 2971 [REDACTED] vulnerability

Do you know when they will get back to you?

[REDACTED] as I'm dealing directly with Bob Gordon and I don't want him getting info from two feeds. Once we have it all sorted out we'll let NCSD know the outcome.

S. Craig Oldham

A/Director General Operations - Directeur général aux opérations intérimaire Government Operations Centre – Centre des opérations du gouvernement Office (613) 991-7728 Secure (613) 996-1088
Cell (613) 299-2114 Craig.Oldham@ps.gc.ca

-----Original Message-----

From: Cameron, Bud
Sent: August 29, 2011 1:45 PM
To: Oldham, Craig
Cc: Schramm, Kent
Subject: FW: Activity 2971 [REDACTED] vulnerability

It seems the fix is available but it is unknown if the clients have been notified, which is what the [REDACTED]
[REDACTED] It is not CCIRC's role to intervene between vendors and researchers. However, we are still looking into it.
Bud

On 11-08-30 02:44 PM, Beaudoin, Luc S wrote:

- This is a valid point, but we both understand that patching process/update is a time consuming exercise, and very few times, and sometimes very unfortunately, are vulnerabilities disclosed publicly prior to their mitigation.

Yes, I did see the plugin....

[REDACTED] for the doc, could you just cut-paste it into an email and mark as private information ? otherwise, I a google account we could use under another email account.

I am interested in looking into this further from a mitigation perspective and maybe collaborate with you to echo your report and rolling this into an eCommerce security best-practice awareness product....

Given the broad range of the vulnerability, theres going to involve a lot of precident setting decisions about who gets notified and the timeframes. Your input would be much appreciated.

--

s.16(2)(c)

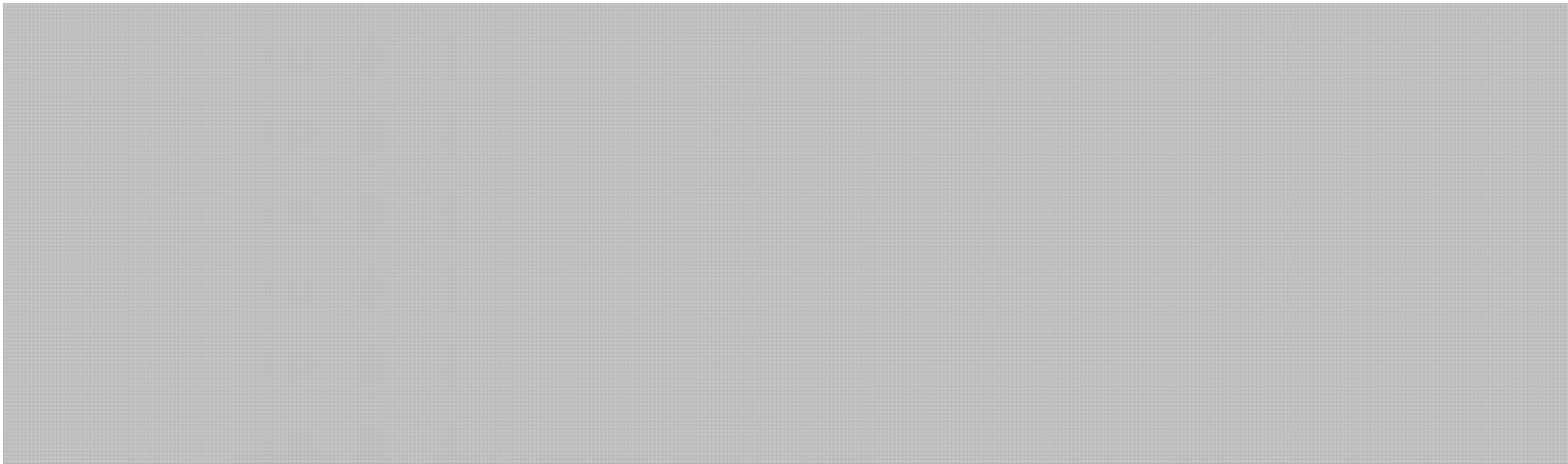
s.19(1)

s.20(1)(c)

Luc

From: [REDACTED]
Sent: August 30, 2011 5:05 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]

[REDACTED]



Luc

s.16(2)(c)

s.19(1)

s.20(1)(c)

From: [redacted]
Sent: August 30, 2011 4:32 PM
To: Beaudoin, Luc S
Subject: Re: [redacted]



s.16(2)(c)

s.19(1)

s.20(1)(c)

On 11-08-30 01:15 PM, Beaudoin, Luc S wrote:

I would like to close the loop with you on your disclosure of the
OPC and PS .

First, thank you for your work with the company and for notifying us. I apologize for not getting back to you sooner. When we received your message, we contacted

Feel free to contact me if you have any question.

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents

cybernétiques

Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

Pages 46 to / à 56
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

s.19(1)
s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Thursday, September 01, 2011 7:09 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]

On 11-09-01 03:53 PM, Beaudoin, Luc S wrote:

try this one:

[REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: Beaudoin, Luc S
Sent: September 1, 2011 2:36 PM
To: [REDACTED]
Subject: RE: [REDACTED]

I will send to you tonight.....so sometimes late afternoon [REDACTED]

thanks again.

Also, I will hopefully be talking tomorrow with [REDACTED] about this.

cheers

Luc

s.19(1)

s.20(1)(c)

From: [REDACTED]
Sent: September 1, 2011 1:06 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]

On 11-08-30 02:44 PM, Beaudoin, Luc S wrote:

[REDACTED]

- This is a valid point, but we both understand that patching process/update is a time consuming exercise, and very few times, and sometimes very unfortunately, are vulnerabilities disclosed publicly prior to their mitigation.

Yes, I did see the [REDACTED]

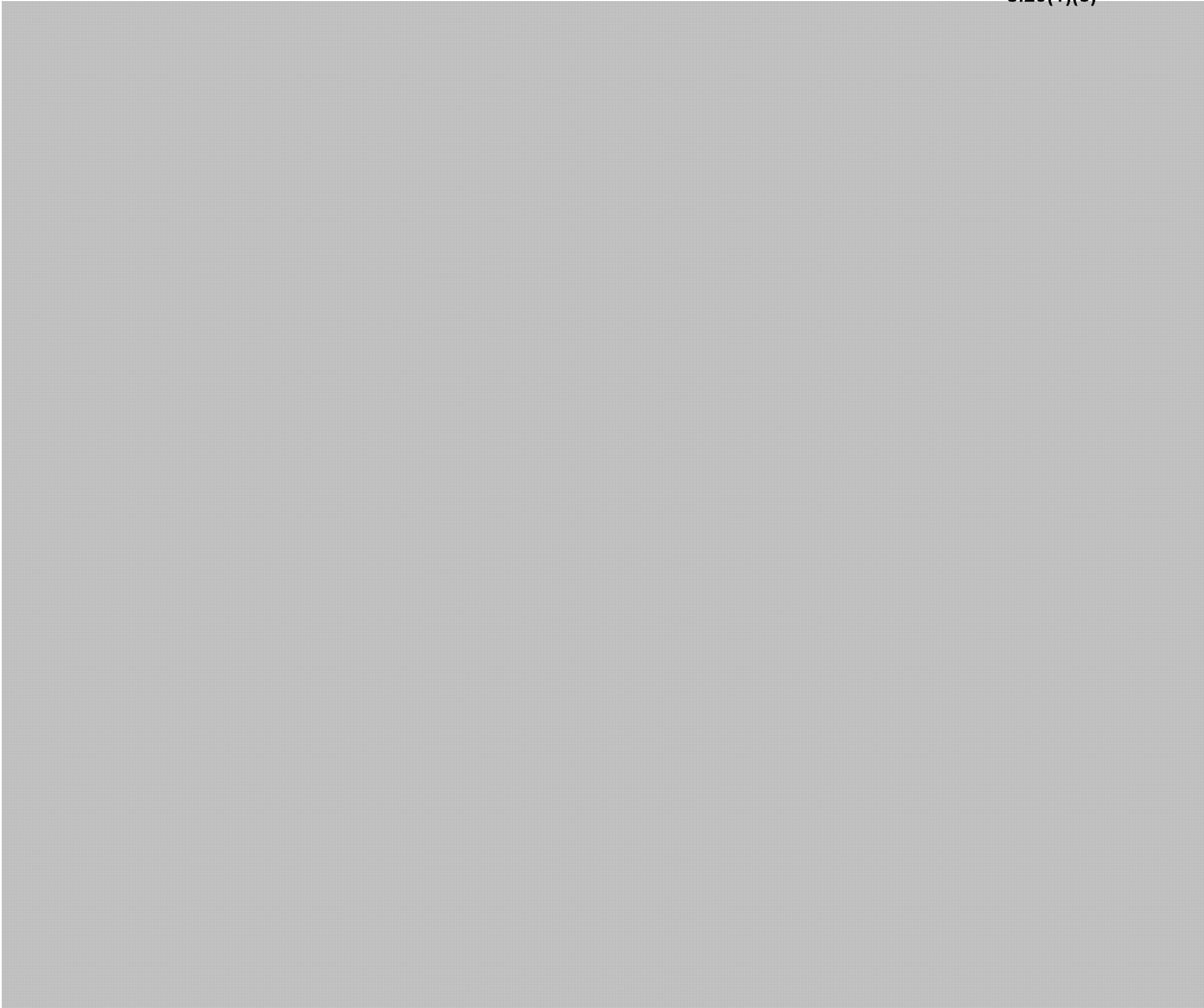
[REDACTED].for the doc, could you just cut-paste it into an email and mark as private information ? otherwise, I a google account we could use under another email account.

I am interested in looking into this further from a mitigation perspective and maybe collaborate with you to echo your report and rolling this into an eCommerce security best-practice awareness product....

cheers

Luc

From: [REDACTED]
Sent: August 30, 2011 5:05 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]



Luc

From: [redacted]
Sent: August 30, 2011 4:32 PM
To: Beaudoin, Luc S
Subject: Re: [redacted]



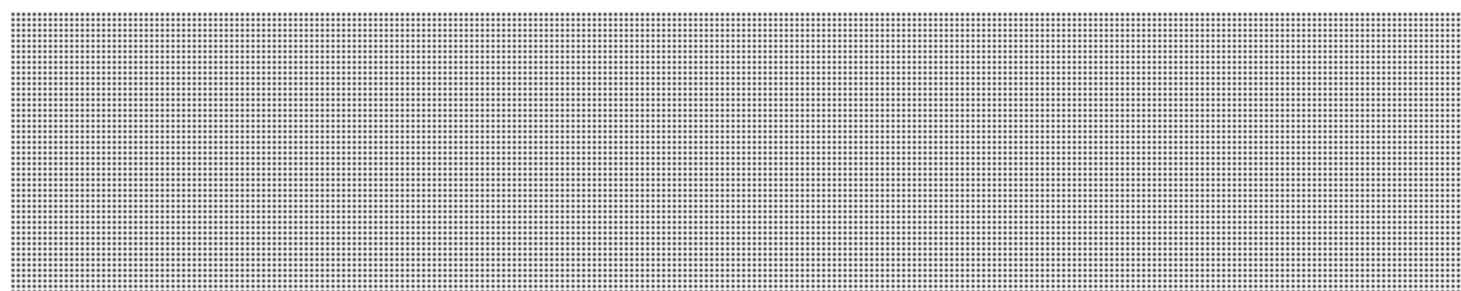


s.16(2)(c)
s.19(1)
s.20(1)(c)

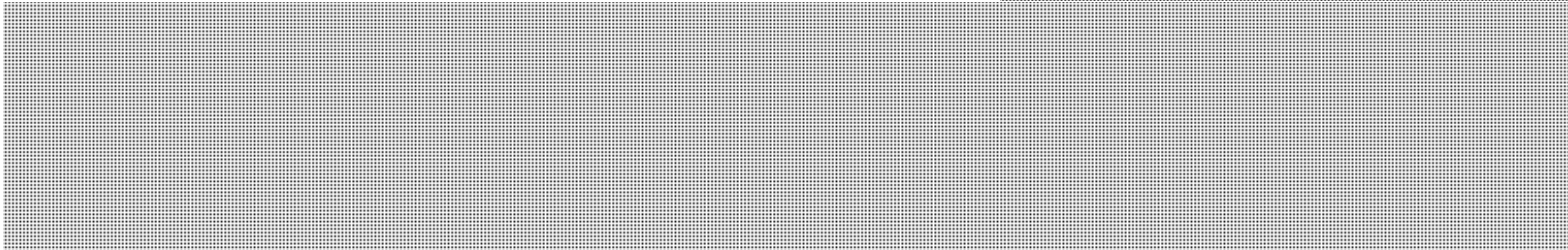
On 11-08-30 01:15 PM, Beaudoin, Luc S wrote:

Hi [redacted]

I would like to close the loop with you on your disclosure of the [redacted]



First, thank you for your work with the company and for notifying us. I apologize for not getting back to you sooner. When we received your message, we contacted [redacted]



Feel free to contact me if you have any question.

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques

cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

app-ann-D-eng.rtf <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

app-ann-D-fra.rtf <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>>

Breault, Stephen

From: [REDACTED]
Sent: Friday, September 02, 2011 6:48 AM
To: Beaudoin, Luc S
Subject: [REDACTED]

Affected Software Identified

DRAFT - The research presented is not yet fully verified and requires further study before vulnerabilities can be confirmed.

Since this document will change as new software is found, I figure a central repository is in order.

To find affected software, look for the presence of CURLOPT_SSL_VERIFYPEER set to 0 or false. This option when set false disables the validation of the SSL certificate and allows for self-signed certificates to be accepted as legitimate.

[REDACTED]

To produce the lists below.

More details on SSL VerifyPeer:

From cURL documentation:

Server Certificates

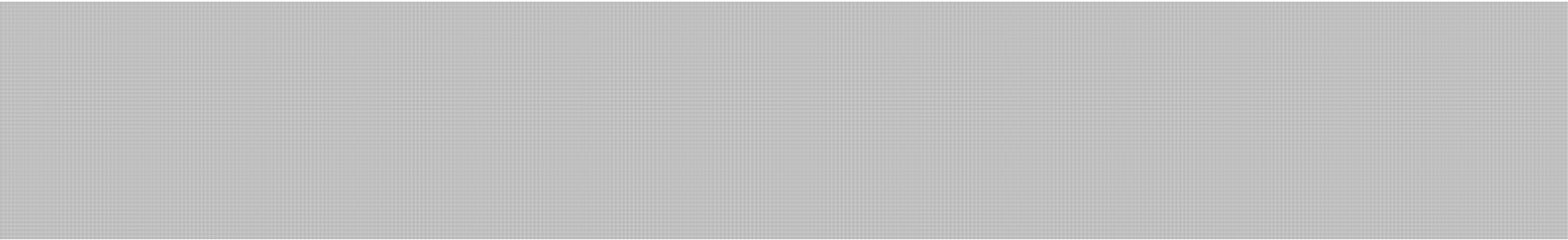
A secure application should never use the CURLOPT_SSL_VERIFYPEER option to disable certificate validation.

There are numerous attacks that are enabled by apps that fail to properly validate server TLS/SSL certificates, thus enabling a malicious server to spoof a legitimate one.

HTTPS without validated certificates is potentially as insecure as a plain HTTP connection.

The following searches are highly useful:

[REDACTED]



Vendors:



Pages 64 to / à 73
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

Breault, Stephen

From: Beaudoin, Luc S
Sent: Friday, September 02, 2011 9:33 AM
To: [REDACTED]
Subject: vulnerability in PHP affecting various sites, including OSCommerce and Moneris....

This is the in-progress/draft research document that [REDACTED] is working on and about which I will be speaking to OPC today.

What is interesting is the use of [REDACTED] to search for potentially affected application.

I want to use this case as a test-case for collaborative security-awareness/research product development....

////////////////////
Affected Software Identified

DRAFT - The research presented is not yet fully verified and requires further study before vulnerabilities can be confirmed.

Since this document will change as new software is found, I figure a central repository is in order.

[REDACTED]

To produce the lists below.

More details on SSL VerifyPeer:

From cURL documentation:

Server Certificates

A secure application should never use the CURLOPT_SSL_VERIFYPEER option to disable certificate validation.

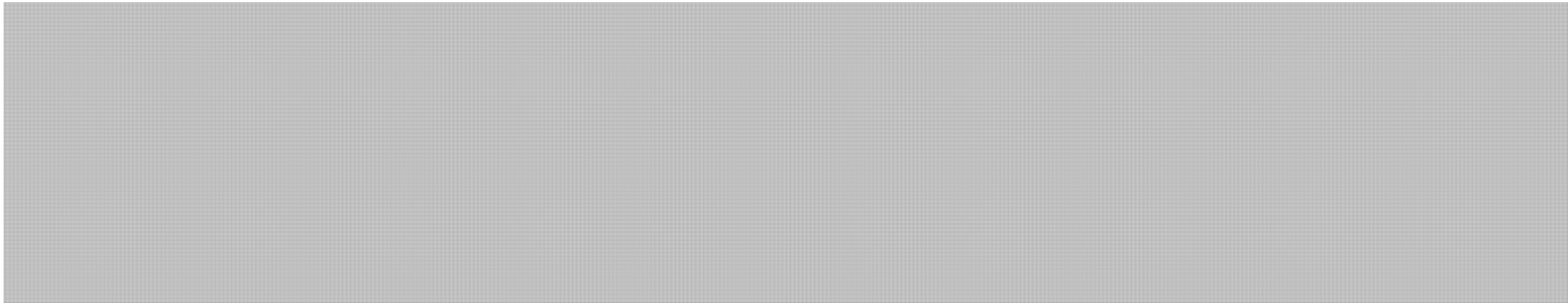
There are numerous attacks that are enabled by apps that fail to properly validate server TLS/SSL certificates, thus enabling a malicious server to spoof a legitimate one.

s.16(1)(b)
s.16(2)(c)

HTTPS without validated certificates is potentially as insecure as a plain HTTP connection.

s.19(1)
s.20(1)(c)

The following searches are highly useful:



Vendors:



Pages 76 to / à 82
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(b)

of the Access to Information
de la Loi sur l'accès à l'information

Page 83

**is withheld pursuant to sections
est retenue en vertu des articles**

16(2)(c), 20(1)(b), 20(1)(c)

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 84 to / à 85
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(b)

of the Access to Information
de la Loi sur l'accès à l'information

Breault, Stephen

From: Beaudoin, Luc S
Sent: Wednesday, September 14, 2011 7:43 PM
To: [REDACTED]
Subject: [REDACTED]

I think we should have a telecon with Ke [REDACTED] and yourself to discuss this issue.

I will contact [REDACTED] tomorrow and confirm they are passing this issue to PS' mitigation. Then, maybe we could discuss the best mechanisms to validate the vulnerability, notify other potentially affected organisations, software providers, and people positioned to mitigate the associated risks.

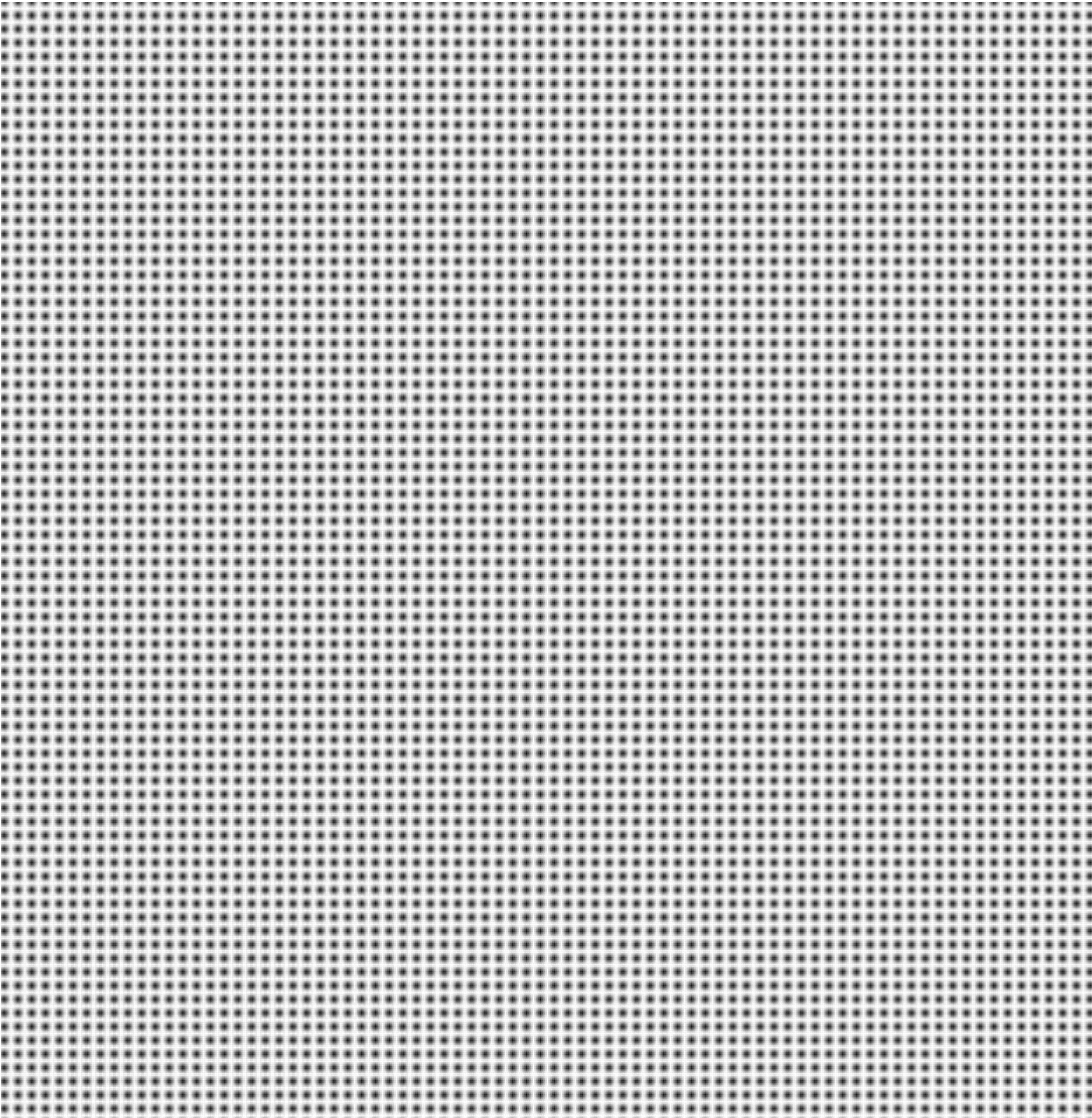
One thing I would like to know is if [REDACTED] has had exchanges with organisations such as [REDACTED] and PHP code project staff about this. The goal being to address not only the current vulnerability instances, but prevent the issue from being reintroduced down the road.

would you be available tomorrow, with [REDACTED] for a teleconference late morning pacific time?

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [REDACTED]
To: Beaudoin, Luc S
Sent: Wed Sep 14 16:44:15 2011
Subject: RE: [REDACTED]



P Do you really need to print this email? / Est-ce nécessaire d'imprimer ce courriel?

From: [REDACTED]
Sent: August 30, 2011 4:32 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]



On 11-08-30 01:15 PM, Beaudoin, Luc S wrote:

[REDACTED]

I would like to close the loop with you on your disclosure of the [REDACTED] to OPC and PS .

First, thank you for your work with the company and for notifying us. I apologize for not getting back to you sooner.

When we received your message, we contacted [REDACTED]

s.16(2)(c)

Feel free to contact me if you have any question.

s.20(1)(c)

Luc

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

Breault, Stephen

From: [REDACTED]
Sent: Thursday, September 15, 2011 11:10 AM
To: [REDACTED]
Subject: RE:

[REDACTED]

From: [REDACTED]
Sent: September 15, 2011 11:09 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: RE:

[REDACTED]

On Sep 15, 2011, at 7:16 AM, [REDACTED] wrote:

12h = 9h PST I think

We can host the teleconference.

[REDACTED] could you please confirm your availability and I will send the phone bridge/confirmation. We can also do webex is needed.

please advise

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

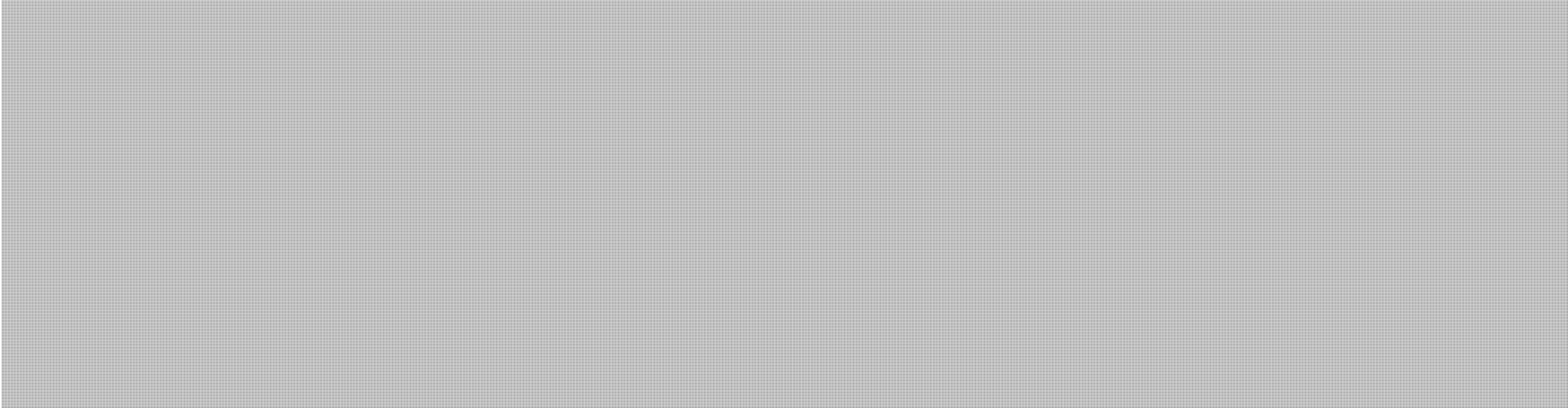
<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>>
<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

s.19(1)

From: [REDACTED]
Sent: September 15, 2011 7:20 AM
To: Beaudoin, Luc S; <<mailto:kevin@stormtide.ca>> kevin@stormtide.ca
Subject: RE:



s.19(1)

s.20(1)(c)

From: Beaudoin, Luc S [<mailto:Luc.Beaudoin@ps-sp.gc.ca>]

Sent: September 15, 2011 7:11 AM

To: [REDACTED]

Subject: Re:

I am good 12h to 13h EST, and 16h to 17h EST...

Luc Beaudoin

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [REDACTED]

To: [REDACTED]

Cc: Beaudoin, Luc S

Sent: Wed Sep 14 19:58:29 2011

Subject: Re:

[REDACTED]

--

[REDACTED]

On 11-09-14 04:56 PM, [REDACTED] wrote:

[REDACTED]

s.19(1)

s.20(1)(c)



P Do you really need to print this email? / Est-ce nécessaire d'imprimer ce courriel?

Breault, Stephen

From: [REDACTED]
Sent: Thursday, September 15, 2011 11:24 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: AC2971: 9h PST ecommerce PHP vulnerability Teleconference details

Please dial in the following phone conference service:

[REDACTED]
Code: [REDACTED]
9h PST, 12h EST

Attendees: [REDACTED] Luc

cheers

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]
Sent: September 15, 2011 10:15 AM
To: [REDACTED]
Subject: RE:

12h = 9h PST I think

We can host the teleconference.

could you please confirm your availability and I will send the phone bridge/confirmation. We can also do webex is needed.

please advise

s.19(1)

Luc

s.20(1)(c)

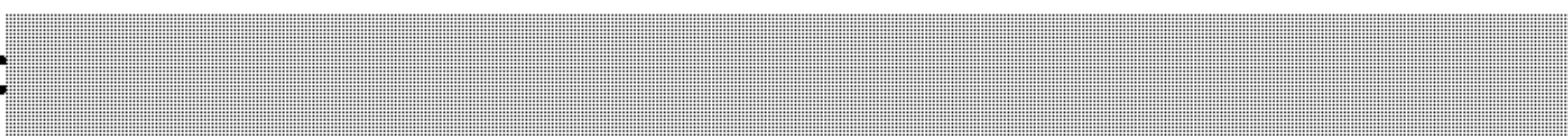
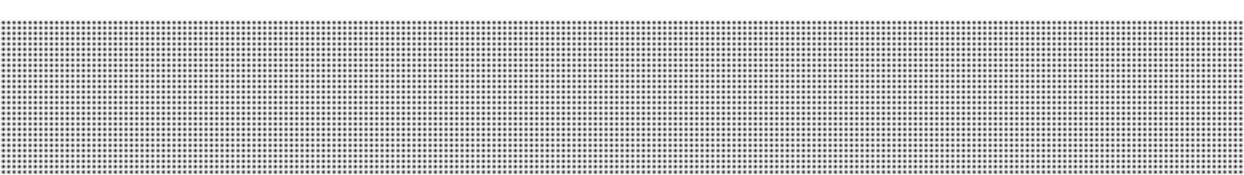
Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

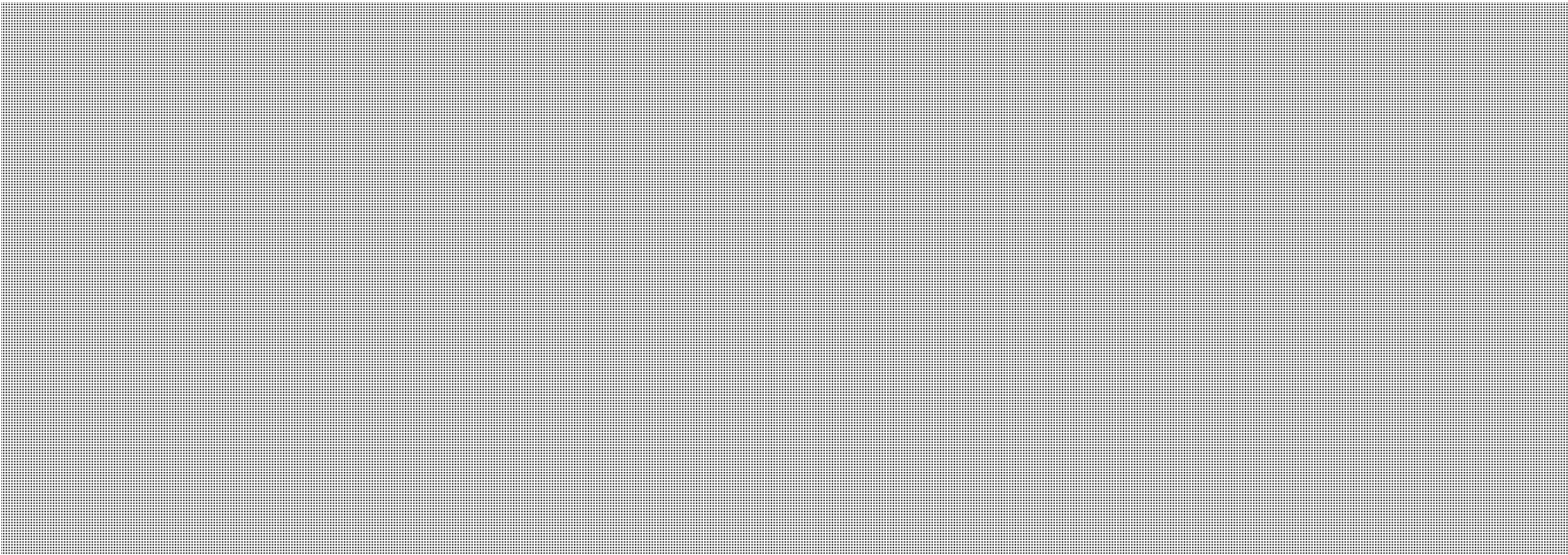
Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: 
Sent: September 15, 2011 7:20 AM
To: Beaudoin, Luc S; 
Subject: RE:



s.19(1)

s.20(1)(c)

From: Beaudoin, Luc S [<mailto:Luc.Beaudoin@ps-sp.gc.ca>]
Sent: September 15, 2011 7:11 AM
To: [REDACTED]
Subject: Re:

I am good 12h to 13h EST, and 16h to 17h EST...

Luc Beaudoin

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [REDACTED]
To: [REDACTED]
Cc: Beaudoin, Luc S
Sent: Wed Sep 14 19:58:29 2011
Subject: Re:

[REDACTED]

On 11-09-14 04:56 PM, [REDACTED] wrote:

[REDACTED]

s.19(1)

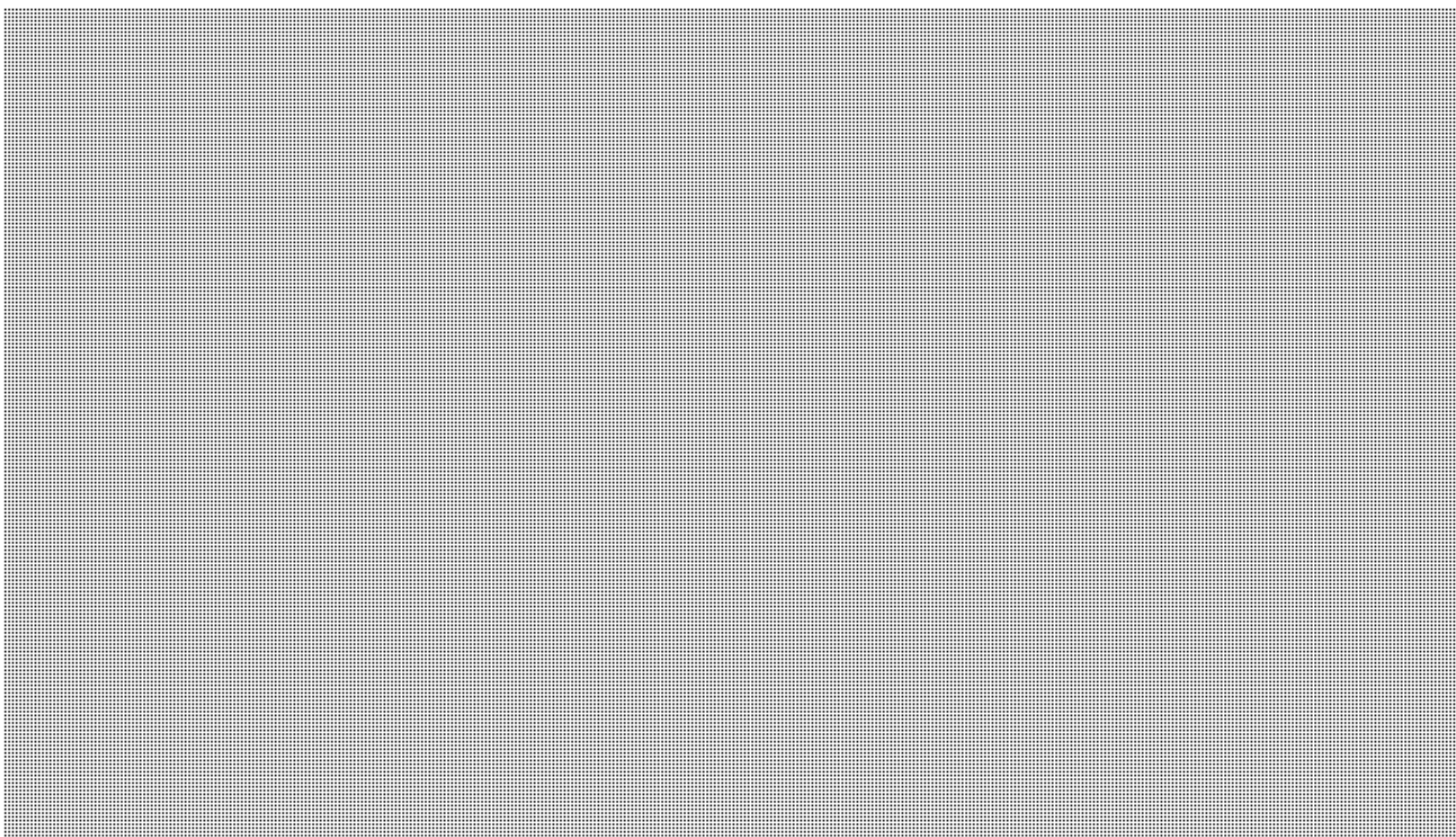
s.20(1)(c)



P Do you really need to print this email? / Est-ce nécessaire d'imprimer ce courriel?

Breault, Stephen

From: [REDACTED]
Sent: Thursday, September 15, 2011 1:29 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: Re: PHP cURL vuln issue: teleconference



On 11-09-15 10:25 AM, Beaudoin, Luc S wrote:

When: September 22, 2011 12:00 PM-1:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where: [REDACTED]

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*~*

Action items before next call:

- [REDACTED]
- We collectively continue building the list of potentially affected products/orgs.
- CCIRC to contact trusted partners to collect initial feedback on this issue
- CCIRC will attempt initial notifications to: [REDACTED]
- [REDACTED]
- CCIRC will send initial request for information to [REDACTED] contact to discuss process further.
- CCIRC will send product template to [REDACTED] : drafting an informational note on this issue.

s.19(1)

Breault, Stephen

From: [REDACTED]
Sent: Thursday, September 15, 2011 1:30 PM
To: Beaudoin, Luc S
Subject: Accepted: PHP cURL vuln issue: teleconference

Breault, Stephen

From: Pitcher Robert
Sent: Wednesday, September 21, 2011 12:00 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC-2971 [REDACTED] potential issue

Roger. Let me shake the tree and see what comes out...

Regards,
Robert Pitcher
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8318
Fax/télécopieur: (613) 996-0995
Email/Courriel: Robert.Pitcher@ps-sp.gc.ca
Website/Site Internet: <http://www.ps-sp.gc.ca> <<http://www.ps-sp.gc.ca/>>

From: Beaudoin, Luc S
Sent: September 21, 2011 10:47 AM
To: Pitcher Robert
Cc: [REDACTED]
Subject: AC-2971 Google shopping cart potential issue

Hi Rob, as discussed, I was wondering if we could get an update from our [REDACTED] wrt the PHP cURL/Verifypeer issue raised by a security researcher in the last month. The issue has to do with the API used by [REDACTED] which may not verify SSL certificate properly for server-to-server connections resulting in sensitive information potentially being passed in the clear.

CCIRC is helping the researcher notify potentially affected organisations/software

The issue was reported to [REDACTED] and is tracked under [REDACTED]

thanks

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

Breault, Stephen

From: Pitcher Robert
Sent: Wednesday, September 21, 2011 12:20 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC-2971 [REDACTED] potential issue

To contextualize, how long have we been looking for an update?

Regards,
Robert Pitcher
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8318
Fax/télécopieur: (613) 996-0995
Email/Courriel: Robert.Pitcher@ps-sp.gc.ca
Website/Site Internet: <http://www.ps-sp.gc.ca> <<http://www.ps-sp.gc.ca/>>

From: Beaudoin, Luc S
Sent: September 21, 2011 10:47 AM
To: Pitcher Robert
Cc: [REDACTED]
Subject: AC-2971 [REDACTED] potential issue

Hi Rob, as discussed, I was wondering if we could get an update from our [REDACTED] wrt the PHP cURL/Verifypeer issue raised by a security researcher in the last month. The issue has to do with the API used by [REDACTED] which may not verify SSL certificate properly for server-to-server connections resulting in sensitive information potentially being passed in the clear.

CCIRC is helping the researcher notify potentially affected organisations/software

The issue was reported to [REDACTED] and is tracked under [REDACTED]

thanks

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

IN11-XXX_CURL_BILINGUAL

La version française suit

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-XXX
Date:

Implementing PHP CURL Verifypeer Option in Applications Requiring SSL Certificate
Verification

PURPOSE
=====

The goal of this Information Note is to raise awareness of a common but potentially insecure implementation of the PHP CURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (CURL or libcurl). The CURL library provides a set of functions that allows establishing connections using various communication protocols including HTTPS. This library is also responsible for implementing security features such as the validation of SSL certificates when establishing HTTPS connections. The CURL library is commonly used by web application developers, particularly in electronic commerce and payment processing applications, to establish secure connections between systems hosted on different network segments, such as connections to third-party payment card processing services.

Within the PHP CURL library, the curl_setopt function allows for the setting of a number of run-time options, including the configuration of how SSL certificates will be verified against relevant Certificate Authorities. The option CURLOPT_SSL_VERIFYPEER defines whether the library will attempt trust validation of SSL certificates when establishing secure connections. When enabled CURL will attempt to verify the remote server's certificate against one or more trusted Certificate Authorities as defined by either of the configuration options CURLOPT_CAINFO or CURLOPT_CAPATH. The CURLOPT_SSL_VERIFYPEER option is enabled by default, and on certain platforms a list of Certificate Authorities is predefined. Unfortunately, this validation framework is often disabled entirely by developers setting the CURLOPT_SSL_VERIFYPEER option to "0" or "false". When peer verification is disabled, SSL certificates are not trust-validated by CURL. Failure of the application to properly validate SSL certificates provides opportunity for a number of man-in-the-middle attack scenarios, potentially leading to interception and modification of data in transit.

The CURL functions are often used for server-to-server communications, and as a result, application operators, such as merchants in electronic commerce, may not be aware that their applications are transacting using potentially unsecured communications channels.

Because software packages are generally provided in source-code, the developer and site operator should ensure security features are enabled according to the sensitivity and expectation of privacy of the data transmitted.

IN11-XXX_CURL_BILINGUAL

SUGGESTED ACTION

=====

CCIRC recommends that operators of web applications that implement TLS/SSL connections for transmitting sensitive information using the PHP CURL library verify that the CURLOPT_SSL_VERIFYPEER option is set to boolean value True, or integer value 1, and ensure failure to return a successful verification results in a failed connection error rather than establishment of an untrusted and unsecured connection. Searching application source code directory for the entries similar to the following will provide indications of the settings used in your CURL implementation:

Examples:

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 0,1,True or False);  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");  
curl_setopt($connection, CURLOPT_CAPATH, "path:/");
```

CCIRC recommends that transaction processing organizations review and ensure that their distributed PHP APIs enforce proper implementation of certificate verification by affiliated merchants and partners accordingly.

Where possible, it is recommended that developers of secure applications PIN certificate validation against the specific CA certificate that will be used. This can be achieved using the CURLOPT_CAINFO option and distributing the associated public CA certificate alongside program code in the same software package. Consult the reference material below for detailed implementation instructions.

CCIRC recommends that operators of web applications regularly verify availability of updates and patches for their software packages, as well as test and deploy these in a timely manner, accordingly.

CREDIT

=====

CCIRC would like to thank Kevin McArthur from StormTide Digital Studios Inc. and Tamir Israel from Canadian Internet Policy and Public Interest Clinic (CIPPIC) for their research and contribution to this product.

References:

=====

```
http://curl.haxx.se/  
http://curl.haxx.se/docs/sslcerts.html  
http://curl.haxx.se/docs/caextract.html  
http://php.net/manual/en/function.curl-setopt.php  
http://www.openssl.org/docs/apps/x509.html  
http://www.openssl.org/docs/ssl/SSL_CTX_load_verify_locations.html
```

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC contributes to the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118

IN11-XXX_CURL_BILINGUAL

Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

NOTE D'INFORMATION

Numéro : IN11-XXX
Date :

Mise en œuvre de l'option Verify Peer de la bibliothèque PHP CURL dans les
applications qui requiert la vérification du certificat SSL

OBJET
=====

La présente note d'information vise à attirer l'attention sur une mise en œuvre courante, mais non sécurisée de l'option CURL PHP utilisée pour vérifier des certificats SSL.

ÉVALUATION
=====

Le langage PHP (préprocesseur hypertexte) est un langage de script côté-serveur adaptable. Il permet au développeur de générer des pages HTML de manière dynamique. Le langage PHP implante plusieurs bibliothèques de codes standards, notamment CURL (Client URL Request Library ou libcurl). Cette dernière comprend un ensemble de fonctions pour établir des connexions avec différents protocoles, dont HTTPS. Elle est également responsable de la mise en place de caractéristiques de sécurité, comme la validation des certificats SSL au moment d'établir des connexions HTTPS. Elle est couramment utilisée par les développeurs d'applications web (p. ex., les applications de commerce et de paiements électroniques) pour établir une connexion sécurisée entre des systèmes hébergés sur différents segments du réseau, notamment la connexion à un service tiers de traitement des cartes de paiement.

Dans la bibliothèque, la fonction curl_setopt permet de régler plusieurs options d'exécution, comme la configuration de la vérification des certificats SSL selon les autorités de certification (AC) pertinentes. L'option CURLOPT_SSL_VERIFYPEER détermine si la bibliothèque va tenter de valider l'approbation des certificats SSL au moment de l'établissement de connexions sécurisées. Lorsque la bibliothèque CURL essaie de vérifier le certificat d'un serveur à distance auprès des AC approuvées conformément à l'option de configuration CURLOPT_CAINFO ou CURLOPT_CAPATH. L'option CURLOPT_SSL_VERIFYPEER est activée par défaut et, sur certaines plateformes, une liste des AC est prédéfinie. Or, ce cadre de validation est souvent désactivé par le développeur qui règle le paramètre de l'option CURLOPT_SSL_VERIFYPEER à « 0 » ou « Faux ». Si la vérification par les pairs est désactivée, les certificats SSL ne sont pas vérifiés pour approbation par la bibliothèque CURL. La non-validation des certificats SSL par l'application ouvre la porte à différents scénarios d'attaque de l'intercepteur (man-in-the-middle attack), ce qui peut mener à l'interception et à la modification des données en transit.

IN11-XXX_CURL_BILINGUAL

Les fonctions CURL sont fréquemment utilisées dans le cadre de communications serveur à serveur et, par conséquent, l'opérateur d'application (p. ex., un marchand qui exploite un commerce électronique) peut ignorer que ses applications font peut-être des transactions sur des canaux de communications non sécurisés.

Les progiciels étant habituellement fournis en code source, le développeur et l'opérateur du site devraient s'assurer que les fonctionnalités de sécurité sont activées conformément à la sensibilité et aux attentes en matière de protection des données transmises.

MESURES RECOMMANDÉES

=====

Le CCRIC recommande aux opérateurs d'applications Web qui mettent en œuvre les connexions TLS/SSL pour la transmission de données sensibles au moyen de la bibliothèque PHP CURL de vérifier que la valeur booléenne de l'option `CURLOPT_SSL_VERIFYPEER` soit réglée à Vrai ou à la valeur correspondant au nombre entier 1 et de régler les paramètres de manière à ce que l'échec d'obtention d'une vérification réussie entraîne une erreur d'échec de connexion plutôt que l'établissement d'une connexion non approuvée et non sécurisée. Il suffit de faire une recherche dans le répertoire de codes sources des applications (voir les exemples d'entrées ci-dessous) pour obtenir des indications sur les paramètres utilisés dans la mise en œuvre CURL :

Exemples :

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 0,1,True or False);  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");  
curl_setopt($connection, CURLOPT_CAPATH, "path:/");
```

Le CCRIC recommande que les organismes qui traitent des transactions examinent leurs API en langage PHP distribuées et qu'ils s'assurent que les API font respecter la mise en œuvre adéquate de la vérification des certificats par les marchands et les partenaires affiliés.

Dans la mesure du possible, les développeurs de NIP d'applications sécurisés doivent certifier la validation selon le certificat d'AC qui sera utilisé. Cela peut être accompli en utilisant l'option `CURLOPT_CAINFO` et en distribuant le certificat public associé de l'AC et le code de programme dans le même progiciel. Veuillez consulter les documents de références ci-dessous pour obtenir des renseignements détaillés sur la mise en œuvre.

Le CCRIC recommande que les opérateurs d'applications Web vérifient régulièrement la disponibilité des mises à jour et des correctifs des progiciels et qu'ils les mettent à l'essai et les déploient adéquatement en temps opportun.

SOURCES

=====

Le CCRIC désire remercier Kevin McArthur de StormTide Digital Studios Inc. et Tamir Israel de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) pour leurs recherches et leur contribution à ce produit.

Références :

=====

```
http://curl.haxx.se/  
http://curl.haxx.se/docs/sslcerts.html  
http://curl.haxx.se/docs/caextract.html  
http://php.net/manual/fr/function.curl-setopt.php  
http://www.openssl.org/docs/apps/x509.html  
http://www.openssl.org/docs/ssl/SSL_CTX_load_verify_locations.html
```

IN11-XXX_CURL_BILINGUAL

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC contribue à la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel :
communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

s.16(2)(c)

s.20(1)(c)

IN11-XXX_EN CURL_VERIFYPEER

La version française suit

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-XXX
Date:

IMPLEMENTATING PHP CURL VERIFYPEER OPTION IN APPLICATIONS REQUIRING SSL CERTIFICATE
VERIFICATION

PURPOSE
=====

The goal of this advisory is to raise awareness of a common but potentially insecure implementation of the PHP CURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (cURL or libcurl). The cURL library provides a set of functions which allow establishing connections using various communication protocols including HTTPS. This library is also responsible for implementing security features such as the validation of SSL certificates when establishing HTTPS connections. The cURL library is commonly used by web application developers, particularly in electronic commerce applications, to establish secure connections between systems hosted on different network segments, such as connections to third-party payment card processing services.

Within the PHP CURL library, the curl_setopt function allows for the setting of a number of run-time options, including the configuration of how SSL certificates will be verified against relevant Certificate Authorities. The option CURLOPT_SSL_VERIFYPEER defines whether the library will attempt trust validation of SSL certificates when establishing secure connections. When enabled CURL will attempt to verify the remote server's certificate against one or more trusted Certificate Authorities as defined by either of the configuration options CURLOPT_CAINFO or CURLOPT_CAPATH. The CURLOPT_SSL_VERIFYPEER option is enabled by default and on certain platforms a list of Certificate Authorities is predefined. Unfortunately, this validation framework is often disabled entirely by developers setting the CURLOPT_SSL_VERIFYPEER option to "0", or "false". When peer verification is disabled, SSL certificates are not trust-validated by CURL. Failure of the application to properly validate SSL certificates provides opportunity for a number of man-in-the-middle attack scenarios potentially leading to interception and modification of data in transit.

The CURL functions are often used for server-to-server communications and as a result application operators, such as merchants in electronic commerce, may not be aware that their applications are transacting using potentially unsecured communications channels.

s.16(2)(c)

s.20(1)(c)

IN11-XXX_EN CURL_VERIFYPEER

and many others. As such software packages are generally provided in source-code, it is the developer's and site operator's role to ensure security features are enabled according to the sensitivity and expectation of privacy of the data transmitted

SUGGESTED ACTION

=====

CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP CURL library, verify that the `CURLOPT_SSL_VERIFYPEER` option is set to boolean value `True`, or integer value `1`, and that failure to return a successful verification results in a failed connection error rather than establishment of an untrusted and unsecured connection. Searching application source code directory for the entries similar to the following will provide indications of the settings used in your CURL implementation:

Examples:

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 0,1,True or False);  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");  
curl_setopt($connection, CURLOPT_CAPATH, "path:/");
```

CCIRC recommends that transaction processing organisations review and ensure that their distributed PHP APIs enforce proper implementation of certificate verification by affiliated merchants and partners accordingly.

Where possible, it is recommended that developers of secure applications pin certificate validation against the specific CA certificate that will be used. This can be achieved using the `CURLOPT_CAINFO` option and distributing the associated public CA certificate alongside program code in the same software package. Consult the reference material below for detailed implementation instructions.

CCIRC recommends that operators of web applications regularly verify availability of updates and patches for their software packages, as well as test and deploy these in a timely manner, accordingly.

CREDIT

=====

CCIRC would like to thank Kevin McArthur from StormTide Digital Studios Inc and Tamir Israel from CIPPIC for their research and contribution to this product.

REFERENCE

=====

- A. <http://curl.haxx.se/>
- B. <http://curl.haxx.se/docs/sslcerts.html>
- C. <http://curl.haxx.se/docs/caextract.html>
- D. <http://php.net/manual/en/function.curl-setopt.php>
- E. <http://www.openssl.org/docs/apps/x509.html>
- F. http://www.openssl.org/docs/ssl/SSL_CTX_load_verify_locations.html

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC contributes to the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

IN11-XXX_EN CURL_VERIFYPEER

For general inquiries into the role of Public Safety Canada, please contact the
department's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589
E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

SÉCURITÉ PUBLIQUE ET PROTECTION CIVILE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

NOTE D'INFORMATION

Numéro : IN11-XXX
Date :

OBJET
=====

ÉVALUATION
=====

Produits touchés :
-

ACTION SUGGÉRÉE
=====

Références :

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point
de convergence au Canada pour les avertissements et l'analyse concernant les menaces
et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse
aux incidents. Le CCRIC contribue à la résilience de l'infrastructure essentielle
nationale en surveillant les menaces et en coordonnant la réponse du gouvernement
fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille
conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité

IN11-XXX_EN CURL_VERIFYPEER

publique Canada, constitue un élément clé de l'approche « tous risques » du
gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des
affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118

Télécopieur : 613-998-9589

Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signa1

IN11-XXX_PHPCURL_VERIFYPEER.txt
La version française suit

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-XXX
Date:

INSECURE IMPLEMENTATIONS OF PHP CURL VERIFYPEER OPTION IN SSL CERTIFICATE
VERIFICATION APPLICATIONS

PURPOSE
=====

The goal of this advisory is to raise awareness of a common but potentially insecure implementation of the PHP CURL option used to verify SSL certificates.

ASSESSMENT
=====

The Client URL library, also known as CURL or libcurl, regroups a set of functions which allow establishing connections using various communication protocols including http, https, ftp, gopher, telnet, dict, file, and ldap. This PHP library can also be used to implement security features such as HTTPS certificates, proxies, cookies and user-password authentication. As a result, the CURL library is commonly used by web application developers, particularly in eCommerce applications, to establish connections between system components hosted on different network segments, such as payment processing service APIs.

The CURL curl_setopt function allows for setting a number of options, including the verification of SSL certificates against relevant Certificate Authority or predefined certificates store bundled with the web application. The option called CURLOPT_SSL_VERIFYPEER, which is set to a value of "1", or "true", by default (from CURL 7.10), enforces the verification of the signing authority for peer certificates presented prior to establishing the SSL connection. Unfortunately, this option is often overridden to "0", or "false", which disables the certificate verification process. This may allow for any self-signed peer certificates to be trusted. As CURL functions are generally used for server to server connections, the owner of the information and the operator of the application server, such as the merchant in an eCommerce application case, may therefore be unaware in the event that an untrusted certificate is presented to establish a connection instead of a valid one. This could be the case for different variants of man-in-the-middle attacks.

The way the CURL library verifies that a peer Certificate is valid is through the use of a list of trusted Certificate Authorities (CA) often called ca-bundle. This list must be populated as a .crt file and referenced accordingly by the developer using the CURLOPT_CAINFO option. Alternatively, the developer may point to specific certificate directory to be used for verification using the CURLOPT_CAPATH option. However, for PEM formatted certificates with OpenSSL, using c_rehash of the directory is required to create appropriate search links.

IN11-XXX_PHPCURL_VERIFYPEER.txt

SUGGESTED ACTION

=====

CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP CURL library, verify that the `CURLOPT_SSL_VERIFYPEER` option is set to `True`, or `"1"`, and that failure to return a successful verification results if a failed connection error rather than establishing an untrusted or insecure connection. Searching application code directory for the entries similar as the following will provide indications of the settings used in your CURL implementation:

Ex:

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 1);
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");
or
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");
```

CCIRC recommends that transaction processing organisation review and ensures their PHP API enforces proper implementation of certificate verification by affiliated merchants and partners.

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:

Telephone: 613-944-4875 or 1-800-830-3118

Fax: 613-998-9589

E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

SÉCURITÉ PUBLIQUE ET PROTECTION CIVILE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

NOTE D'INFORMATION

Numéro : IN11-XXX

Date :

OBJET

=====

IN11-XXX_PHPCURL_VERIFYPEER.txt

ÉVALUATION

=====

Produits touchés :

-

ACTION SUGGÉRÉE

=====

Références :

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents. Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118

Télécopieur : 613-998-9589

Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signal

La version française suit

Formatted: Font color: Black

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-XXX
Date:

INSECURE IMPLEMENTATIONS OF PHP CURL VERIFYPEER OPTION IN
APPLICATIONS REQUIRING SSL CERTIFICATE VERIFICATION
APPLICATIONS

PURPOSE
=====

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, French (Canada)

The goal of this advisory is to raise awareness of a common but potentially insecure implementation of the PHP cURL option used to verify SSL certificates.

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, French (Canada)

Formatted: Font color: Black

ASSESSMENT
=====

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, French (Canada)

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (cURL or libcurl). The cURL library provides a set of functions which allow establishing connections using various communication protocols including HTTPS. This library is also responsible for implementing security features such as the validation of SSL certificates when establishing HTTPS connections. The cURL library is commonly used by web application developers, particularly in electronic commerce applications, to establish secure connections between systems hosted on different network segments, such as connections to third-party payment card processing services.

Within the PHP cURL library, the curl_setopt function allows for the setting of a number of run-time options, including the configuration of how SSL certificates will be verified against relevant Certificate Authorities. The option CURLOPT_SSL_VERIFYPEER defines whether the library will attempt trust validation of SSL certificates when establishing secure connections. When enabled cURL will attempt to verify the remote server's certificate against one or more trusted Certificate Authorities as defined by either of the configuration options CURLOPT_CAINFO or CURLOPT_CAPATH. The

s.16(2)(c)
s.20(1)(c)

CURLOPT_SSL_VERIFYPEER option is enabled by default and on certain platforms a list of Certificate Authorities is predefined. Unfortunately, this validation framework is often disabled entirely by developers setting the CURLOPT_SSL_VERIFYPEER option to "0", or "false". When peer verification is disabled, SSL certificates are not trust-validated by cURL. Failure of the application to properly validate SSL certificates provides opportunity for a number of man-in-the-middle attack scenarios potentially leading to interception and modification of data in transit.

The cURL functions are generally used for server-to-server communications and as a result application operators, such as merchants in electronic commerce, may not be aware that their applications are transacting using potentially unsecured communications channels.



SUGGESTED ACTION
=====

CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP cURL library, verify that the CURLOPT_SSL_VERIFYPEER option is not set to boolean value false, or integer value 0, and that failure to return a successful verification results in a failed connection error rather than establishment of an untrusted and unsecured connection. Searching application source code directory for the entries similar to the following will provide indications of the settings used in your cURL implementation:

Examples:

- Formatted: English (U.S.)
- Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)
- Formatted: English (U.S.)
- Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)
- Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)
- Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)
- Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)
- Formatted: Font color: Black, French (Canada)
- Formatted: Font color: Black, French (Canada)
- Formatted: Font color: Black, French (Canada)
- Formatted: Font color: Black, French (Canada)
- Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, French (Canada)

curl_setopt(\$connection, CURLOPT_SSL_VERIFYPEER, 1);
curl_setopt(\$connection, CURLOPT_SSL_VERIFYPEER, 0);
curl_setopt(\$connection, CURLOPT_SSL_VERIFYPEER, true);
curl_setopt(\$connection, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt(\$connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");
curl_setopt(\$connection, CURLOPT_CAINFO, "path:/ca.pem");
curl_setopt(\$connection, CURLOPT_CAPATH, "path:/");

Specifically the strings "CURLOPT_SSL_VERIFYPEER", "CURLOPT_CAINFO" and "CURLOPT_CAPATH" should be searched.

CCIRC recommends that transaction processing organisations review and ensure that their distributed PHP APIs enforce proper implementation of certificate verification by affiliated merchants and partners accordingly.

Where possible, it is recommended that developers of secure applications pin certificate validation against the specific CA certificate that will be used. This can be achieved using the CURLOPT_CAINFO option and distributing the associated public CA certificate alongside program code in the same software package.

CCIRC recommends that operators of web applications regularly verify availability of updates and patches for their software packages, as well as test and deploy these in a timely manner, accordingly.

Formatted: English (U.S.)

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)

CREDIT
=====

CCIRC would like to thank Kevin McArthur from StormTide Digital Studios Inc and Tamir Israel from CIPPIC for their research and contribution to this product.

PURPOSE
=====

The goal of this advisory is to raise awareness of a common but potentially insecure implementation of the PHP cURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Processor (PHP) is a flexible server side scripting language and environment. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including cURL. The Client URL library, also known as cURL or libcurl, regroups a set of functions which allow establishing connections using various communication protocols including http, https, ftp, gopher, telnet, dict, file, and ldap. This PHP library can also be used to implement security features such as HTTPS certificates, proxies, cookies and user password authentication. As a result, the cURL library is commonly used by web application developers, particularly in eCommerce applications, to establish connections between system components hosted on different network segments, such as payment processing service APIs.

The cURL curl_setopt function allows for setting a number of options, including the verification of SSL certificates against relevant Certificate Authority or predefined certificates store bundled with the web application. The option called CURLOPT_SSL_VERIFYPEER, which is set to a value of "1", or "true", by default (from cURL 7.10), enforces the verification of the signing authority for peer certificates presented prior to establishing the SSL connection. Unfortunately, this option is often overridden to "0", or "false", which disables the certificate verification process. This may allow for any self-signed peer certificates to be trusted. As cURL functions are generally used for server to server connections, the owner of the information and the operator of the application server, such as the merchant in an eCommerce application case, may therefore be unaware in the event that an untrusted certificate is presented to establish a connection instead of a valid one. This could be the case for different variants of man in the middle attacks.

Formatted: English (U.S.)
Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, English (U.S.)
Formatted: Font color: Black, English (U.S.)
Formatted: Font color: Black

The way the cURL library verifies that a peer Certificate is valid is through the use of a list of trusted Certificate Authorities (CA) often called ca bundle. This list must be populated as a .crt file and referenced accordingly by the developer using the CURLOPT_CAINFO option. Alternatively, the developer may point to a specific certificate directory to be used for verification using the CURLOPT_CAPATH option. However, for PEM formatted certificates with OpenSSL, using c_rehash of the directory is required to create appropriate search links.

Comment [P1]: Is is the OpenSSL c_rehash function and what do you have to do to the directory?

Formatted: Font color: Black

Formatted: Font color: Black

SUGGESTED ACTION

CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP cURL library, verify that the CURLOPT_SSL_VERIFYPEER option is set to True, or "1", and that failure to return a successful verification results in a failed connection error rather than establishing an untrusted or insecure connection. Searching application code directory for the entries similar as the following will provide indications of the settings used in your cURL implementation:

Ex:

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 1);  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");  
or  
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");
```

Formatted: Font color: Black, English (U.S.)

CCIRC recommends that transaction processing organisation review and ensures their PHP API enforces proper implementation of certificate verification by affiliated merchants and partners.

Formatted: Font color: Black

Note to Readers

The Canadian Cyber Incident Response Centre (CCIRC) provides a focal point for Canada's cyber threat and vulnerability warning, analysis and response. CCIRC is responsible for assuring the resilience of national critical infrastructure through monitoring threats and coordinating a federal response to cyber security incidents of national interest. CCIRC operates in conjunction with the Government Operations Centre (GOC) within Public Safety Canada and is a key component of the government's all-hazards approach to emergency management and national security.

For general inquiries into the role of Public Safety Canada, please contact the department's Public Affairs division at:
Telephone: 613-944-4875 or 1-800-830-3118
Fax: 613-998-9589

Turbide, Frank

From: Beaudoin, Luc S
Sent: September-22-11 5:36 PM
To: Turbide, Frank
Cc: Bendelier, Kenneth
Subject: php first stab for comments
Attachments: IN11-XXX_PHPCURL_VERIFYPEER.txt

reference activity 2971

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

E-mail: communications@ps-sp.gc.ca

For urgent matters or to report any incidents, please contact the GOC.

SÉCURITÉ PUBLIQUE ET PROTECTION CIVILE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

NOTE D'INFORMATION

Numéro : IN11-XXX
Date :

OBJET
=====

ÉVALUATION
=====

Produits touchés :

-

ACTION SUGGÉRÉE
=====

Références :

Note aux lecteurs

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) constitue le point de convergence au Canada pour les avertissements et l'analyse concernant les menaces et les vulnérabilités cybernétiques, ainsi que pour la coordination de la réponse aux incidents.

Le CCRIC est chargé d'assurer la résilience de l'infrastructure essentielle nationale en surveillant les menaces et en coordonnant la réponse du gouvernement fédéral aux incidents de cybersécurité d'intérêt national. Le CCRIC, qui travaille conjointement avec le Centre des opérations du gouvernement (COG) de Sécurité publique Canada, constitue un élément clé de l'approche « tous risques » du gouvernement en regard de la gestion des urgences et de la sécurité nationale.

Pour obtenir des renseignements généraux, veuillez communiquer avec la Division des affaires publiques de Sécurité publique Canada :

Téléphone : 613-944-4875 ou 1-800-830-3118

Télécopieur : 613-998-9589

Courriel : communications@ps-sp.gc.ca

En cas de questions urgentes, ou pour signal

Breault, Stephen

From:

s.16(2)(c)

Sent:

Friday, September 30, 2011 11:09 AM

s.19(1)

To:

Beaudoin, Luc S

s.20(1)(c)

Cc:

Subject:

Re: teleconference today: postpone

On 11-09-30 07:29 AM, Beaudoin, Luc S wrote:

I will be unable to dial in today for our scheduled weekly teleconference. I would like to invite you to resume our discussions next Thursday, 12h.

Update: We have not heard back from [REDACTED] this time. We have confirmed that the information had been shared properly caveated from [REDACTED]

[REDACTED] We have also engaged with [REDACTED] to request opinion of the appropriateness of a CVE for this case. We have not received a response yet.

Finally, please consider the draft advisory below. I would very much appreciate an opinion on the content, references and credit, as you would see appropriate.

again, my apologies for today s cancellation.

Cheers

////////DRAFT, not for public release////////

INFORMATION NOTE

Number: IN11-XXX

Date:

INSECURE IMPLEMENTATIONS OF PHP CURL VERIFYPEER OPTION IN APPLICATIONS REQUIRING SSL CERTIFICATE VERIFICATION

PURPOSE

=====

The goal of this advisory is to raise awareness of a common but potentially insecure implementation of the PHP cURL option used to verify SSL certificates.

ASSESSMENT

=====

The PHP Hypertext Processor (PHP) is a flexible server-side scripting language and environment. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including cURL. The Client URL library, also known as cURL or libcurl, regroups a set of functions which allow establishing connections using various communication protocols including http, https, ftp, gopher, telnet, dict, file, and ldap. This PHP library can also be used to implement security features such as HTTPS certificates, proxies, cookies and user-password authentication. As a result, the cURL library is commonly used by web application developers, particularly in eCommerce

applications, to establish connections between system components hosted on different network segments, such as payment processing service APIs.

The cURL `curl_setopt` function allows for setting a number of options, including the verification of SSL certificates against relevant Certificate Authorities or predefined certificates store bundled with the web application. The option called `curl_setopt_ssl_verifypeer`, which is set to a value of "1", or "true", by default (██████████) enforces the verification of the signing authority for peer certificates presented prior to establishing the SSL connection. Unfortunately, this option is often overridden to "0", or "false", which disables the certificate verification process. This may allow for any self-signed peer certificates to be trusted. As cURL functions are generally used for server to server connections, the owner of the information and the operator of the application server, such as the merchant in an eCommerce application case, may therefore be unaware in the event that an untrusted certificate is presented to establish a connection instead of a valid one. This could be the case for different variants of man-in-the-middle attacks.

The way the cURL library verifies that a peer Certificate is valid is through the use of a list of trusted Certificate Authorities (CA) often called ca-bundle. This list must be populated as a .crt file and referenced accordingly by the developer using the `CURLOPT_CAINFO` option. Alternatively, the developer may point to a specific certificate directory to be used for verification using the `curl_setopt_capath` option. However, for PEM formatted certificates with OpenSSL, using `c_rehash` of the directory is required to create appropriate search links.

SUGGESTED ACTION

=====

CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP cURL library, verify that the `curl_setopt_ssl_verifypeer` option is set to True, or "1", and that failure to return a successful verification results in a failed connection error rather than establishing an untrusted or insecure connection. Searching application code directory for the entries similar as the following will provide indications of the settings used in your cURL implementation:

Ex:

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 1);
```

```
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");
```

or

```
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");
```

CCIRC also recommends that transaction, or other sensitive personal information, processing organisations review and ensure their PHP API enforces proper implementation of certificate verification by affiliated merchants and partners.

s.19(1)

Credit

([REDACTED] ? Others ? references ?)

////////////////////////////////////

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

Breault, Stephen

Subject: PHP cURL vuln issue: teleconference
Location:

Start: Fri 9/30/2011 12:00 PM
End: Fri 9/30/2011 1:00 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Beaudoin, Luc S
Required Attendees:

When: September 30, 2011 12:00 PM-1:00 PM (GMT-05:00) Eastern Time (US & Canada).
Where:

Note: The GMT offset above does not reflect daylight saving time adjustments.

~~*~*~*~*~*~*~*

This is FRIDAY instead of THURSDAY (I have a schedule conflict), if a problem let me know

Action items before next call:

- CCIRC follow up with
- CCIRC rapidly follow up with to validate non-disclosure broad developer community
- CCIRC notification to as next priority.
- CCIRC teleconf with : provide result and way ahead
- CCIRC to provide draft advisory for your comments
- We collectively continue building the list of potentially affected products/orgs.

Turbide, Frank

From: Bendelier, Kenneth
Sent: October-03-11 10:05 AM
To: Beaudoin, Luc S; Pitcher Robert; Turbide, Frank
Subject: RE: 2971: Notification PHP cURL VERIFYPEER use in [REDACTED]

What's a PHP? Pre-Hewlett-Packard?

-----Original Message-----

From: Beaudoin, Luc S
Sent: October 3, 2011 10:01 AM
To: Pitcher Robert; Turbide, Frank; Bendelier, Kenneth
Cc: [REDACTED]
Subject: 2971: Notification PHP cURL VERIFYPEER use [REDACTED]

Frank and Ken: how does this sound ?
Rob: trusted contact for [REDACTED]

To: [REDACTED]

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of PHP APIs using your services. CCIRC would like to raise awareness of this issue and seek your support in mitigating any associated risks.

Various implementations of the PHP cURL library use the SSL_VERIFYPEER option set to FALSE. These implementations may result in incomplete verification of your services' SSL certificates, potentially making the communication channel vulnerable to man-in-the-middle attacks.

Specifically, the following [REDACTED] may lead to incomplete certificate validation:

Module:

[REDACTED]

Details:

Sets curl_setopt(\$ch, CURLOPT_SSL_VERIFYPEER, 0);

Module:

[REDACTED]

Module:

[REDACTED]

As these modules are used for server to server communication, the user may be unaware that personal information provided using the browser over a proper SSL connection may be further transmitted insecurely.

The appropriate use of PHP cURL library for verifying peer certificate prior to establishing an SSL connection would implement the following:

- Set CURLOPT_SSL_VERIFYPEER to "True" or "1";
- Set CURLOPT_CAINFO to appropriate certificate bundle filepath;

- In case of failure to verify certificate, ie VERIFY_PEER returns False, do not establish the connection and generate appropriate log message.

In order to limit the risk of inappropriate disclosure of personal information, CCIRC recommends that APIs to your services make appropriate use of SSL certificate verification mechanisms and ensure that failed verification does not result in the transmission of personal information insecurely.

CCIRC would like to work with your organisation to identify potentially affected implementations and develop effective mitigations accordingly.

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

Breault, Stephen

From: Turbide, Frank
Sent: Monday, October 03, 2011 10:53 AM
To: Beaudoin, Luc S; Pitcher Robert; Bendelier, Kenneth
Cc: [REDACTED]
Subject: RE: 2971: Notification PHP cURL VERIFYPEER use [REDACTED]

You didn't like my PHP paragraph? :(

-----Original Message-----

From: Beaudoin, Luc S
Sent: October 3, 2011 10:01 AM
To: Pitcher Robert; Turbide, Frank; Bendelier, Kenneth
Cc: [REDACTED]
Subject: 2971: Notification PHP cURL VERIFYPEER use [REDACTED]

Frank and Ken: how does this sound ?

Rob: trusted contact [REDACTED]

To [REDACTED]

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of PHP APIs using your services. CCIRC would like to raise awareness of this issue and seek your support in mitigating any associated risks.

Various implementations of the PHP cURL library use the SSL_VERIFYPEER option set to FALSE. These implementations may result in incomplete verification of your services' SSL certificates, potentially making the communication channel vulnerable to man-in-the-middle attacks.

Specifically, the following [REDACTED] may lead to incomplete certificate validation:

Module:

[REDACTED]

Details:

Sets curl_setopt(\$ch, CURLOPT_SSL_VERIFYPEER, 0);

Module:

[REDACTED]

Module:

[REDACTED]

As these modules are used for server to server communication, the user may be unaware that personal information provided using the browser over a proper SSL connection may be further transmitted insecurely.

The appropriate use of PHP cURL library for verifying peer certificate prior to establishing an SSL connection would implement the following:

- Set CURLOPT_SSL_VERIFYPEER to "True" or "1";

- Set CURLOPT_CAINFO to appropriate certificate bundle filepath;
- In case of failure to verify certificate, ie VERIFY_PEER returns False, do not establish the connection and generate appropriate log message.

In order to limit the risk of inappropriate disclosure of personal information, CCIRC recommends that APIs to your services make appropriate use of SSL certificate verification mechanisms and ensure that failed verification does not result in the transmission of personal information insecurely.

CCIRC would like to work with your organisation to identify potentially affected implementations and develop effective mitigations accordingly.

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

s.16(2)(c)

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Monday, October 03, 2011 11:53 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: 2971: Notification [REDACTED]
Importance: High

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of APIs which are used to access your services. CCIRC would like to raise your awareness of this potential issue and seek your support in mitigating any associated risks.

Could you confirm who might be the most appropriate contact in [REDACTED] to disclose the technical details surrounding this issue to (API applications development team maybe ?) and the associated PGP key (if different than the one found here [REDACTED])

thank you

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

Breault, Stephen

From: Beaudoin, Luc S
Sent: Monday, October 03, 2011 12:08 PM
To: Turbide, Frank
Subject: RE: 2971: Notification PHP cURL VERIFYPEER use in [REDACTED]

Ack. Addressed by sending a primer first requesting contact and changing text to "used to access your services...."

Luc Beaudoin, P.Eng, MSc, MBA
 Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
 canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
 Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
 Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

-----Original Message-----

From: Turbide, Frank
 Sent: October 3, 2011 11:03 AM
 To: Beaudoin, Luc S
 Subject: RE: 2971: Notification PHP cURL VERIFYPEER use in [REDACTED]

1. Who will get this notification? Will they know enough to forward it to the appropriate individual?
2. "using your services"... 'while using your services' or 'used by your services'?

-----Original Message-----

From: Beaudoin, Luc S
 Sent: October 3, 2011 10:01 AM
 To: Pitcher Robert; Turbide, Frank; Bendelier, Kenneth
 Cc: [REDACTED]
 Subject: 2971: Notification PHP cURL VERIFYPEER use in [REDACTED]

Frank and Ken: how does this sound ?

Rob: trusted contact for [REDACTED]

To [REDACTED]

Breault, Stephen

From: Beaudoin, Luc S
Sent: Monday, October 03, 2011 1:10 PM
To: Pitcher Robert
Subject: RE: 2971: Notification PHP cURL VERIFYPEER use [REDACTED]

Roger that. I sent a primer

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

-----Original Message-----

From: Pitcher Robert
Sent: October 3, 2011 10:24 AM
To: Beaudoin, Luc S; Turbide, Frank; Bendelier, Kenneth
Cc: [REDACTED] Cameron, Bud
Subject: RE: 2971: Notification PHP cURL VERIFYPEER use [REDACTED]

I don't have a personal contact [REDACTED] The one you have below is the only one I am aware of. [REDACTED]

[REDACTED]

Might be a good start to fire them a request for a research/developer department instead of unloading the technical data on them below. I mean you pretty much spell it out to them below the vulnerability. Considering the content, this information should probably be encrypted to a pgp address. So if we report that we have a significant vulnerability we wish to inform them of, it should result in 2 way communication. Can't see why they wouldn't want to work with us on this...

Regards,
Robert Pitcher
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8318

s.16(2)(c)

s.20(1)(c)

Fax/télécopieur: (613) 996-0995
Email/Courriel: Robert.Pitcher@ps-sp.gc.ca
Website/Site Internet: <http://www.ps-sp.gc.ca>

-----Original Message-----

From: Beaudoin, Luc S
Sent: October 3, 2011 10:01 AM
To: Pitcher Robert; Turbide, Frank; Bendelier, Kenneth
Cc: [REDACTED]
Subject: 2971: Notification PHP cURL VERIFYPEER use [REDACTED]

Frank and Ken: how does this sound ?
Rob: trusted contact for [REDACTED]

[REDACTED]

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of PHP APIs using your services. CCIRC would like to raise awareness of this issue and seek your support in mitigating any associated risks.

Various implementations of the PHP cURL library use the SSL_VERIFYPEER option set to FALSE. These implementations may result in incomplete verification of your services' SSL certificates, potentially making the communication channel vulnerable to man-in-the-middle attacks.
Specifically, the following PayPal PHP SDK may lead to incomplete certificate validation:

Module:

[REDACTED]
Details:

Sets curl_setopt(\$ch, CURLOPT_SSL_VERIFYPEER, 0);

Module:

[REDACTED]
Module:

[REDACTED]

As these modules are used for server to server communication, the user may be unaware that personal information provided using the browser over a proper SSL connection may be further transmitted insecurely.

The appropriate use of PHP cURL library for verifying peer certificate prior to establishing an SSL connection would implement the following:

- Set CURLOPT_SSL_VERIFYPEER to "True" or "1";
- Set CURLOPT_CAINFO to appropriate certificate bundle filepath;
- In case of failure to verify certificate, ie VERIFY_PEER returns False, do not establish the connection and generate appropriate log message.

In order to limit the risk of inappropriate disclosure of personal information, CCIRC recommends that APIs to your services make appropriate use of SSL certificate verification mechanisms and ensure that failed verification does not result in the transmission of personal information insecurely.

s.16(2)(c)

s.20(1)(c)

[REDACTED] notification (2)

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of PHP APIs using your services. CCIRC would like to raise awareness of this issue and seek your support in mitigating any associated risks.

Various implementations of the PHP CURL library use the SSL_VERIFYPEER option set to FALSE. These implementations may result in incomplete verification of your services' SSL certificates, potentially making the communication channel vulnerable to man-in-the-middle attacks. Specifically, the following [REDACTED] may lead to incomplete certificate validation:

Module:

[REDACTED]
Details:

Sets curl_setopt(\$ch, CURLOPT_SSL_VERIFYPEER, 0);

Module:

[REDACTED]
Module:

As these modules are used for server to server communication, the user may be unaware that personal information provided using the browser over a proper SSL connection may be further transmitted insecurely.

The appropriate use of PHP CURL library for verifying peer certificate prior to establishing an SSL connection would implement the following:

- Set CURLOPT_SSL_VERIFYPEER to "True" or "1";
- Set CURLOPT_CAINFO to appropriate certificate bundle filepath;
- In case of failure to verify certificate, ie VERIFY_PEER returns False, do not establish the connection and generate appropriate log message.

In order to limit the risk of inappropriate disclosure of personal information, CCIRC recommends that APIs to your services make appropriate use of SSL certificate verification mechanisms and ensure that failed verification does not result in the transmission of personal information insecurely.

CCIRC would like to work with your organisation to identify potentially affected implementations and develop effective mitigations accordingly.

[REDACTED]

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of PHP APIs using your services. CCIRC would like to raise awareness of this issue and seek your support in mitigating any associated risks.

Various implementations of the PHP CURL library use the SSL_VERIFYPEER option set to FALSE. These implementations may result in incomplete verification of your services' SSL certificates, potentially making the communication channel vulnerable to man-in-the-middle attacks. Specifically, the following [REDACTED] implementations may lead to incomplete certificate validation:

Note: Recommended PHP APIs [REDACTED]

[REDACTED]

Module:

[REDACTED]

Details:

[REDACTED]

Code:

```
$this->request->setConfig('ssl_verify_peer', false);
```

This code has the following comment:

[REDACTED]

Module

[REDACTED]

Module:

[REDACTED]

Details:

[REDACTED]

Code and comments:

```
/* Verify SSL Cert. */  
public $ssl_verifypeer = FALSE;  
curl_setopt($ci, CURLOPT_SSL_VERIFYPEER, $this->ssl_verifypeer);
```

Module:

[REDACTED]

Code Details:

[REDACTED]

```
curl_setopt($ch, CURLOPT_CAINFO, $cert);  
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, true);
```

s.16(2)(c)

s.20(1)(c)

```
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 2);  
}  
else  
{  
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);  
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);  
}
```

Breault, Stephen

From: Beaudoin, Luc S
Sent: Monday, October 03, 2011 3:05 PM
To: Pitcher Robert
Subject: RE: POC for [REDACTED]

it is the SSL thing. Yes, I think you should ping your contact. The content is as follow, which I need to massage into a custom notification:

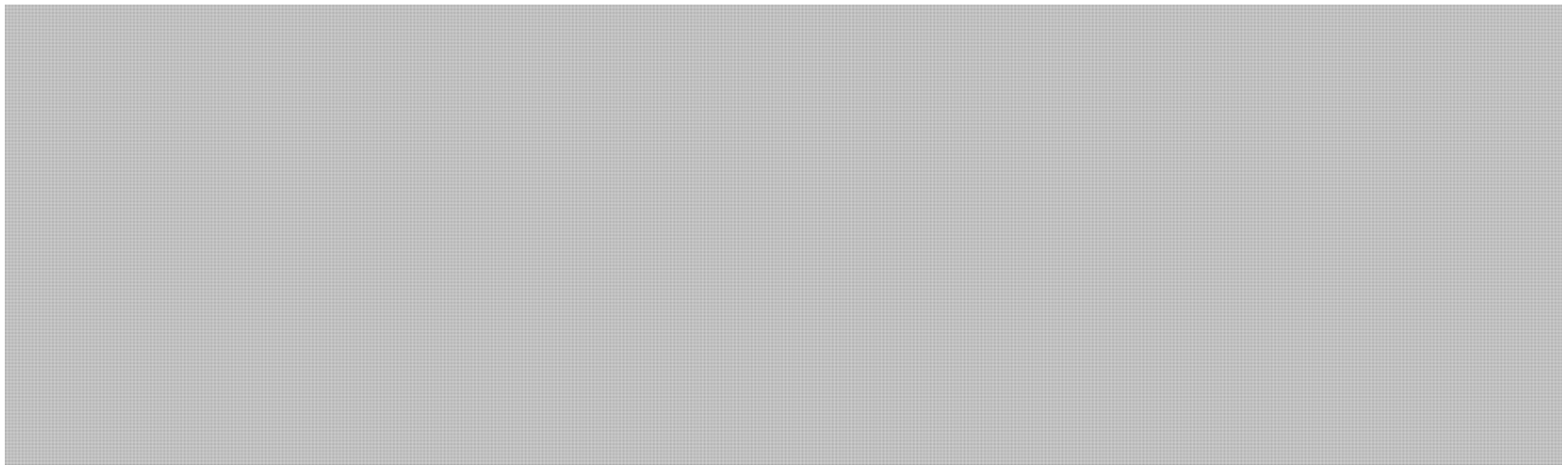


Has comment of:

// XXX ssl won't work with ssl_verify_peer set to true, which is

// the default in HTTP_Request2

Vulnerable to verifypeer.



s.16(2)(c)

s.20(1)(c)

// you probably don't want to change any of these curl values

'curl_connecttimeout' => 30,

'curl_timeout' => 10,

// for security you may want to set this to TRUE. If you do you need

// to install the servers certificate in your local certificate store.

'curl_ssl_verifypeer' => false,

Vulnerable by default however can be configured to be secure. Author acknowledges security consideration.

/* Verify SSL Cert. */

public \$ssl_verifypeer = FALSE;

curl_setopt(\$ci, CURLOPT_SSL_VERIFYPEER, \$this->ssl_verifypeer);

Again can be configured to be secure, but is insecure by default. Comment at least makes it known that the setting controls the ssl certificate verification to the user.

Secure by default. Ships a ca-bundle.crt file, thus by-passing the system installed defaults, however, it appears to be a sane list of trusted ca's. If that file is deleted or cannot be read, then the ssl checks are bypassed rather than failing.

```
// if the certificate exists then use it, else bypass ssl checks

if(file_exists($cert = dirname(__FILE__) . DIRECTORY_SEPARATOR . 'ca-bundle.crt'))
{
    curl_setopt($ch, CURLOPT_CAINFO, $cert);

    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, true);

    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 2);
}

else
{
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, false);
}
```

s.16(2)(c)

s.20(1)(c)

s.16(2)(c)

s.20(1)(c)

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: Pitcher Robert
Sent: October 3, 2011 3:03 PM
To: Beaudoin, Luc S
Subject: RE: POC for [REDACTED]

Assume this is all related to the SSL thing? I can hit up the name if you want me too, but if you think it's not appropriate now, let me know.

From: Beaudoin, Luc S
Sent: October 3, 2011 3:00 PM
To: Pitcher Robert
Subject: RE: POC for [REDACTED]

[REDACTED] has a vulnerability disclosure form on their website, but I think this is not the appropriate way for us to do this. Here is the message I wanted to send them:

//////////

The Canadian Cyber Incident Response Centre (CCIRC) was recently informed of potentially insecure implementations of APIs which are used to access your services. CCIRC would like to raise your awareness of this potential issue and seek your support in mitigating any associated risks.

Could you confirm who might be the most appropriate contact at [REDACTED] to disclose the technical details surrounding this issue to (API applications development team maybe ?) and the associated PGP key, if available ?

s.16(2)(c)

thank you

s.20(1)(c)

//////////

Any help would be great. Otherwise, I will send to a generic input email address.... [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: Pitcher Robert

s.16(1)(b)

s.16(2)(c)

s.20(1)(c)

Sent: October 3, 2011 2:14 PM

To: Beaudoin, Luc S

Subject: RE: POC for [REDACTED]

I have a name, but don't think I personally know him. I can approach him however under [REDACTED]
[REDACTED] Lemmie know.

Regards,

Robert Pitcher

Canadian Cyber Incident Response Centre

Phone/téléphone: (613) 949-8318

Fax/télécopieur: (613) 996-0995

Email/Courriel: Robert.Pitcher@ps-sp.gc.ca

Website/Site Internet: <http://www.ps-sp.gc.ca> <<http://www.ps-sp.gc.ca/>>

From: Beaudoin, Luc S

Sent: October 3, 2011 1:16 PM

To: Pitcher Robert

Subject: POC for [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

Breault, Stephen

From: [REDACTED] s.16(2)(c)
Sent: Monday, October 03, 2011 5:07 PM s.19(1)
To: [REDACTED] s.20(1)(c)
Subject: Re: 2971: Notification [REDACTED] potential security issue
Importance: High

Luc,

I am unable to find out who owns the key that is listed on the [REDACTED]
Can you send again and encrypt using this key? Thanks.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.1



-----END PGP PUBLIC KEY BLOCK-----

s.16(2)(c)

s.19(1)

s.20(1)(c)

On 10/3/11 11:32 AM, [REDACTED]

>Thanks for the quick reply. Find details attached (pgp'd using [REDACTED]
>key). We would appreciate your thoughts on this.

>

>Cheers

>

>Luc Beaudoin, P.Eng, MSc, MBA

>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>Cyber Incident Response Centre | Centre canadien de réponse aux

>incidents cybernétiques Public Safety Canada | Sécurité publique Canada

>Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1

>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of

>Canada | Gouvernement du Canada

>

>

>Need to report an incident? Find the Incident Report Form here:

>

>

><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/it>

>imp

>-pgimti-app-ann-D-eng.rtf

>

>Vous voulez rapporter un incident ? Utilisez le formulaire de

>déclaration

>suivant:

>

><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/it>

>imp

>-pgimti-app-ann-D-fra.rtf

>

>

>

>

>-----Original Message-----

>From: [REDACTED]

>Sent: October 3, 2011 12:22 PM

>To: [REDACTED]

>Subject: Re: 2971: Notification [REDACTED] potential security issue

>Importance: High

>

>Luc,

>

>I am a member of the Security Operations Center [REDACTED] Please

>provide more information in regards to your discovery. Thanks.

>

>

s.16(2)(c)

s.19(1)

s.20(1)(c)

>
>From: ([REDACTED])
>Date: Mon, 3 Oct 2011 09:52:37 -0600
>To: ([REDACTED])
>Subject: 2971: Notification [REDACTED] potential security issue
>
>The Canadian Cyber Incident Response Centre (CCIRC) was recently
>informed of potentially insecure implementations of APIs which are used
>to access your services. CCIRC would like to raise your awareness of
>this potential issue and seek your support in mitigating any associated risks.
>
>Could you confirm who might be the most appropriate contact [REDACTED]
>to disclose the technical details surrounding this issue to (API
>applications development team maybe ?) and the associated PGP key (if
>different than the one found here
[REDACTED]
>
>thank you
>
>Luc Beaudoin, P.Eng, MSc, MBA
>Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>Cyber Incident Response Centre | Centre canadien de réponse aux
>incidents cybernétiques Public Safety Canada | Sécurité publique Canada
>Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1
>613-991-3574 luc.beaudoin@ps-sp.gc.ca<mailto:luc.beaudoin@ps-sp.gc.ca>
>PublicSafety.gc.ca
>Government of Canada | Gouvernement du Canada
>
>
>Need to report an incident? Find the Incident Report Form here:
>
>
><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
>
>Vous voulez rapporter un incident ? Utilisez le formulaire de

>déclaration

>suivant:

>

><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/it>

>imp

>-pgimti-app-ann-D-fra.rtf<<http://www.tbs-sct.gc.ca/sim-gsi/publications>

>/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>

>

>

Breault, Stephen

From: Beaudoin, Luc S
Sent: Tuesday, October 04, 2011 11:09 AM
To: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

Sensitivity: Confidential

now is good

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

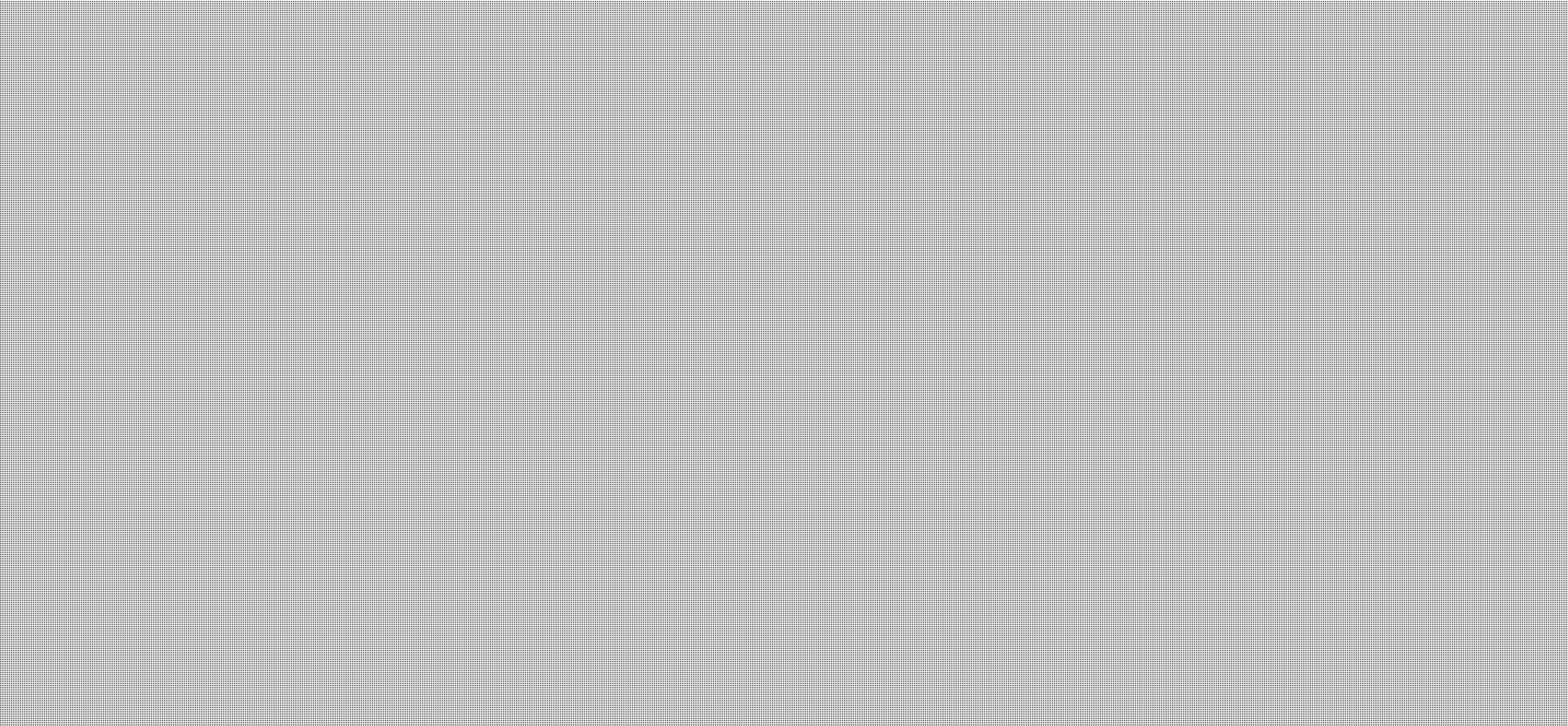
From: [REDACTED]
Sent: October 4, 2011 11:06 AM
To: Beaudoin, Luc S; [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential

Yes,

Luc, are you or your team available to have a discussion on this and if so when?

Regards,

s.20(1)(c)

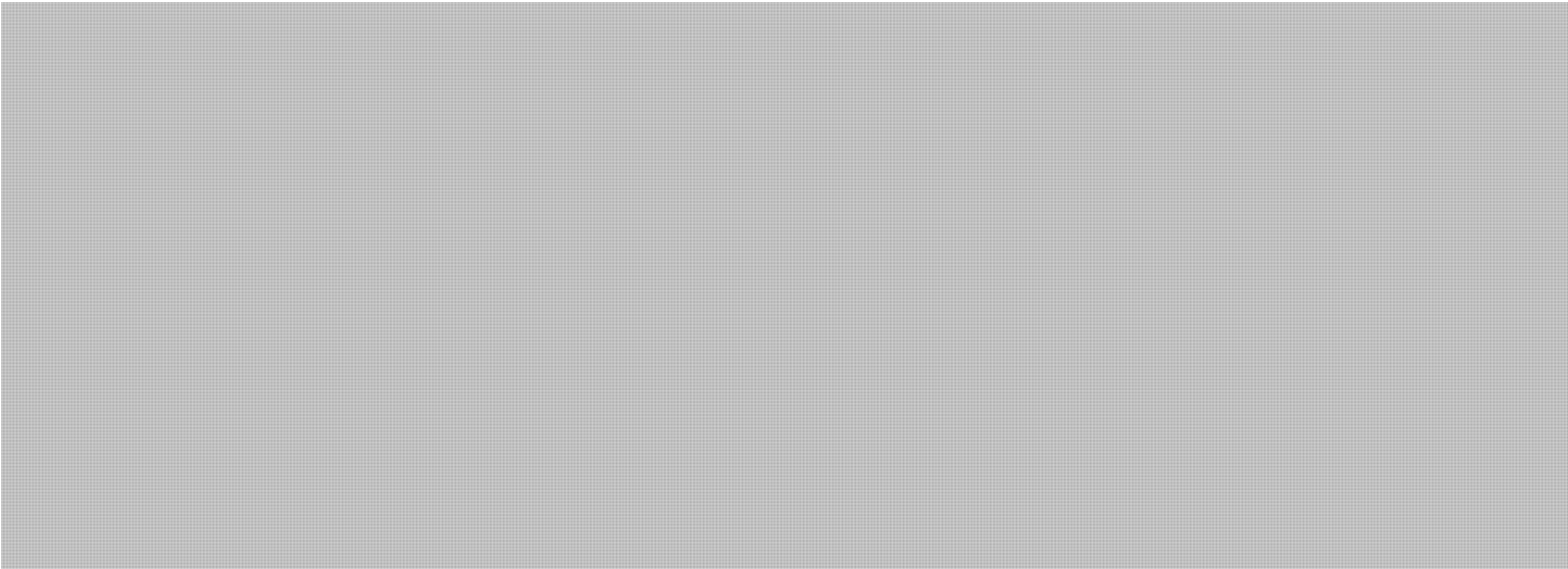


Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: [REDACTED]
Sent: October 4, 2011 10:55 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential



From: [redacted]
Sent: October 4, 2011 10:50 AM
To: [redacted]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential



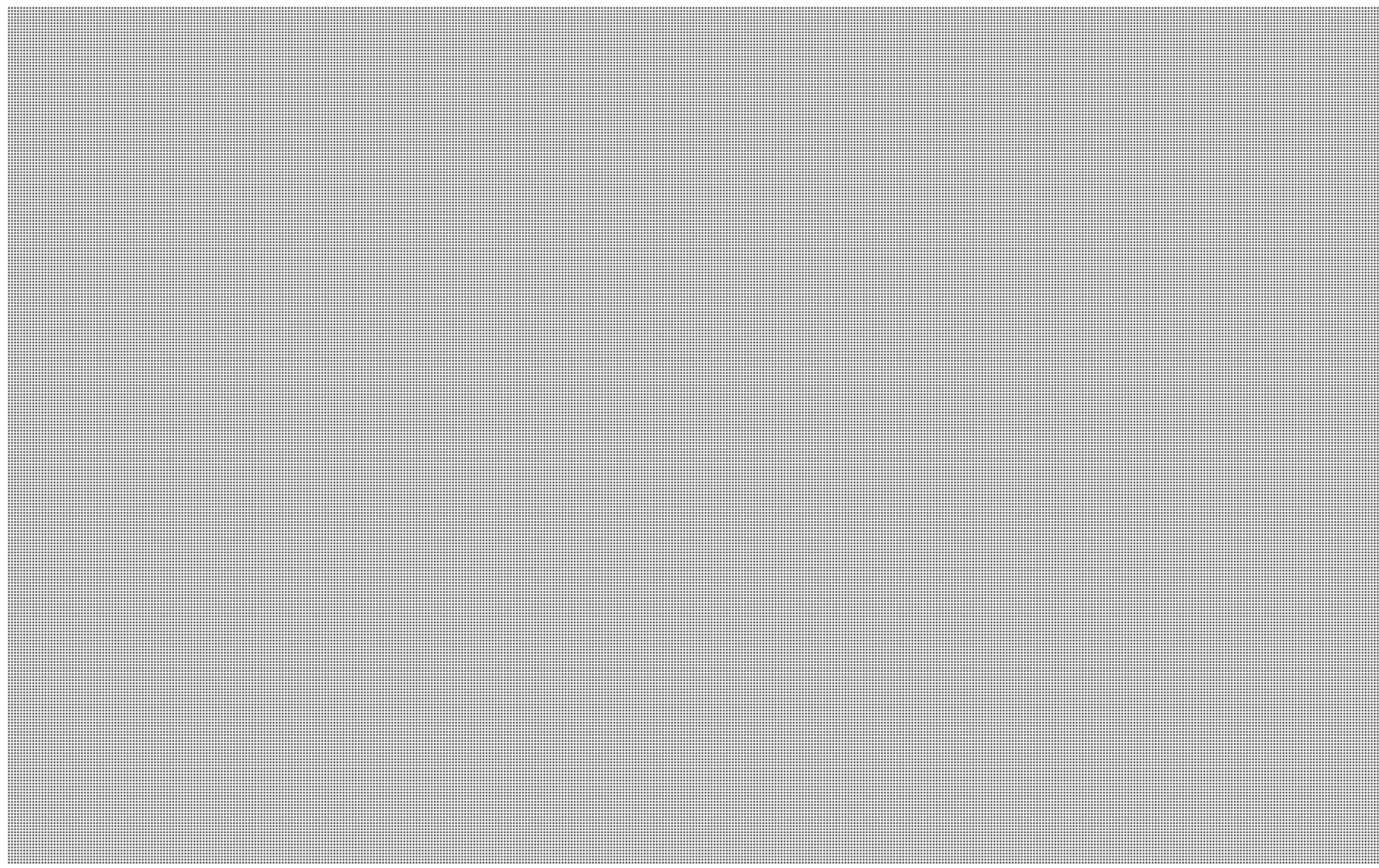
Pages 153 to / à 156
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

s.16(2)(c)

s.20(1)(c)



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 19, 2011 4:47 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

PROTECTED

Limited Distribution

[REDACTED] is one we know has an API with [REDACTED] and seems to display this issue. But again, these are merchant-side apps and may not be used at all by [REDACTED]. Most likely, the team looking at on-line services / eCommerce for [REDACTED] would have an idea of the API concerned. The concern is that potentially private information like credit card data be exchanged in the clear where the user expects it to be SSL all the way.

thanks alot again...

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]
Sent: September 19, 2011 4:24 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

Hi Luc,

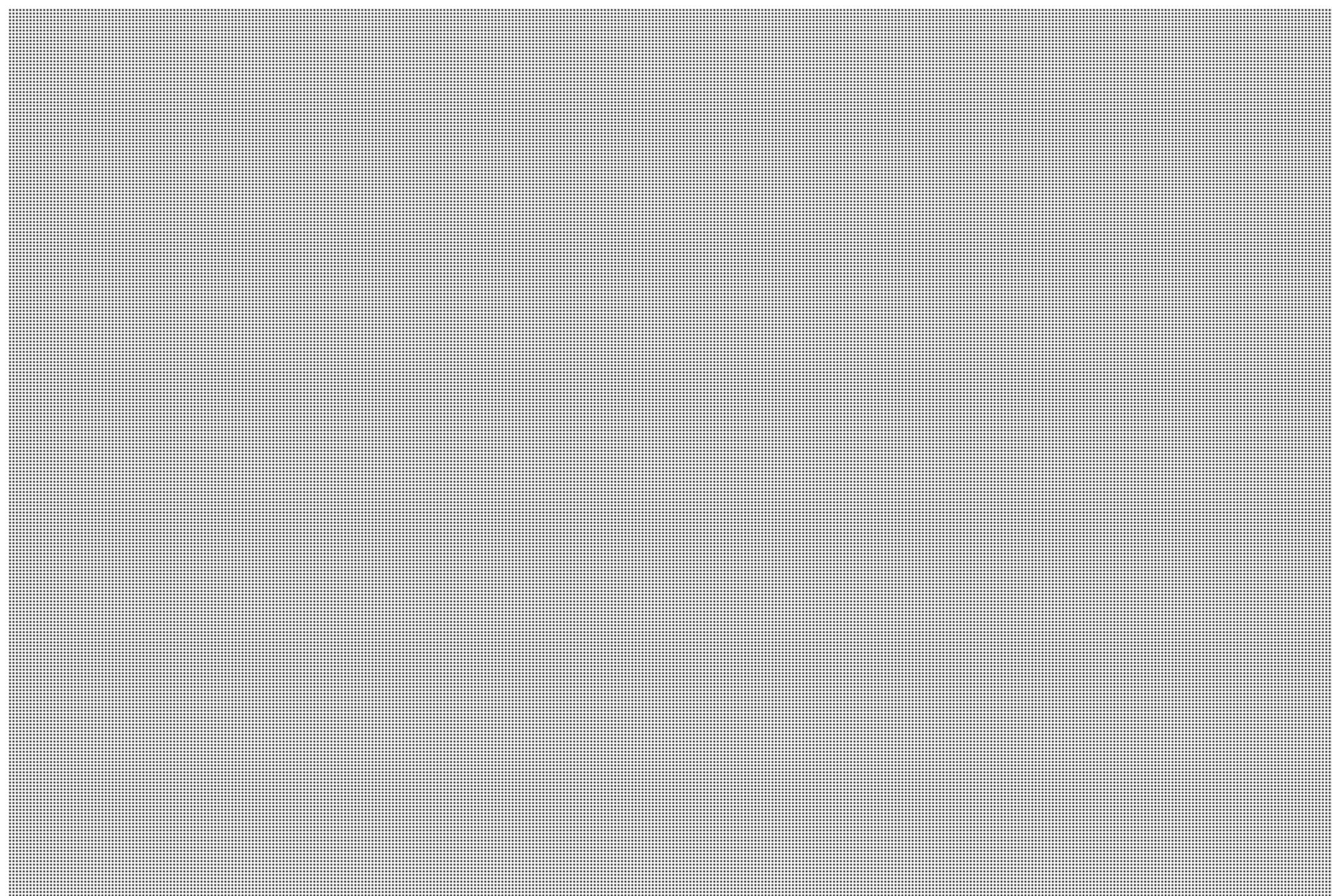
I am still trying to get information on this issue. Do you have a particular app/web you can point to?

Regards,

[REDACTED]

s.16(2)(c)

s.20(1)(c)



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 16, 2011 11:39 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

PROTECTED

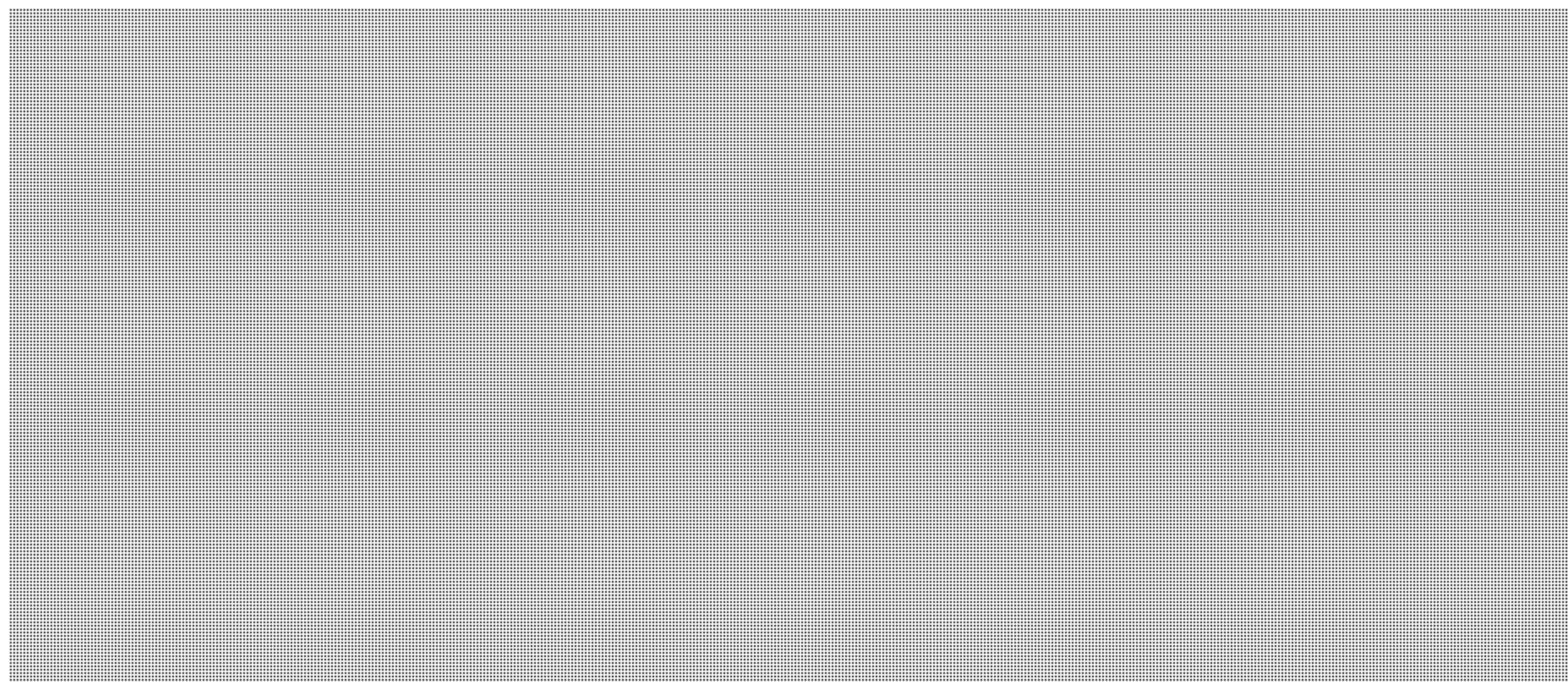
Limited Distribution (within Need to Know Technical Staff of your organisation)

The issue is reported in PHP implementation of cURL options for certificate check in SSL transaction between 2 servers (generally between merchant and transaction processor) . Specifically, a software package called [REDACTED] amongst others, implements a [REDACTED] which seems to be affected. Here are some details:

CURLOPT_SSL_VERIFYPEER seems turned off in [REDACTED] accepting self-signed certificates, or maybe even defaulting back to HTTP. This exposes data to Man-in-The-Middle attacks.

Module:

s.16(2)(c)



Question:

- What would these API be used for ?
- Do you know how prevalent is [REDACTED] amongst your merchants ?
- Do you know if [REDACTED] expects merchant applications to properly authenticate SSL connections ?

thanks for your help

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

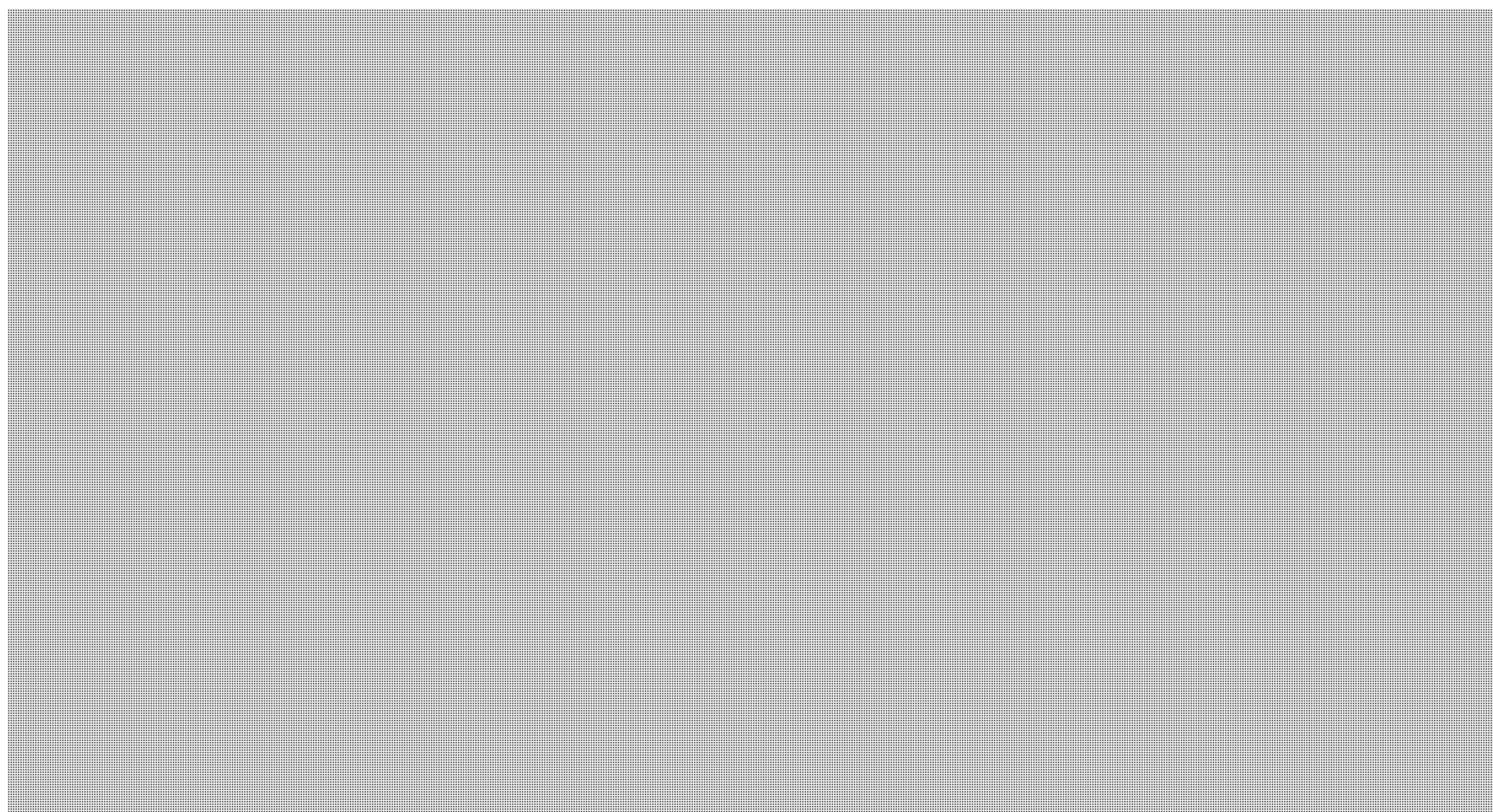
s.16(2)(c)

From: [REDACTED]
Sent: September 16, 2011 10:44 AM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

Hi Luc,

As per my voice mail, would it be possible to send more detail as to the particular app?

Regards,



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 15, 2011 5:25 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: AC2971 contact for PHP based ecommerce site

s.16(2)(c)

Hi Mark,

I am trying to locate someone in [REDACTED] who might be involved with the online store applications used to process on-line payments by affiliated merchants. I beleive there is an API the group uses which leverages PHP cURL and certificate options for which we are researching a potential vulnerability/configuration issue.

any help would be great.

cheers

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Tuesday, October 04, 2011 11:13 AM
To: Beaudoin, Luc S
Cc: Pitcher Robert
Subject: Re: [REDACTED] for unsecure api issue

On Tue, Oct 4, 2011 at 6:06 AM, Beaudoin, Luc S <Luc.Beaudoin@ps-sp.gc.ca> wrote:

> Thanks Rob.

>

[REDACTED] we were contacted by a researcher about potential incorrect certificate verification for SSL by some APIs for
[REDACTED] We normally send these using PGP. Do you have a key ?

>

> Luc

>

>

> Luc Beaudoin, P.Eng, MSc, MBA

> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

> Cyber Incident Response Centre | Centre canadien de réponse aux

> incidents cybernétiques Public Safety Canada | Sécurité publique

> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur

> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government

> of Canada | Gouvernement du Canada

>

>

> Need to report an incident? Find the Incident Report Form here:

>

>

> <http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/i>

> timp-pgimti-app-ann-D-eng.rtf

>

> Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

s.16(2)(c)

>

s.19(1)

> <http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/i>

s.20(1)(c)

> timp-pgimti-app-ann-D-fra.rtf

>

>

> -----Original Message-----

> From: Pitcher Robert

> Sent: October 3, 2011 4:39 PM

> To: [REDACTED] Beaudoin, Luc S

> Subject: [REDACTED] for unsecure api issue

>

> Luc,

>

> Allow me to introduce [REDACTED] ead [REDACTED] He should be able to assist you with the issue you are working on regarding api issues.

>

[REDACTED]
>

> Luc is the operations manager here at the CCIRC. I'll leave it to him to explain the technical details of the issue he is working on.

>

> Cheers,

> Rob

>

>

Breault, Stephen

From: Beaudoin, Luc S
Sent: Tuesday, October 04, 2011 11:50 AM
To: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential

reviewing the email chain, we may not need to have a teleconference. Would you guys happen to have a trusted contact with [REDACTED] we could use to discuss this issue with ?

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

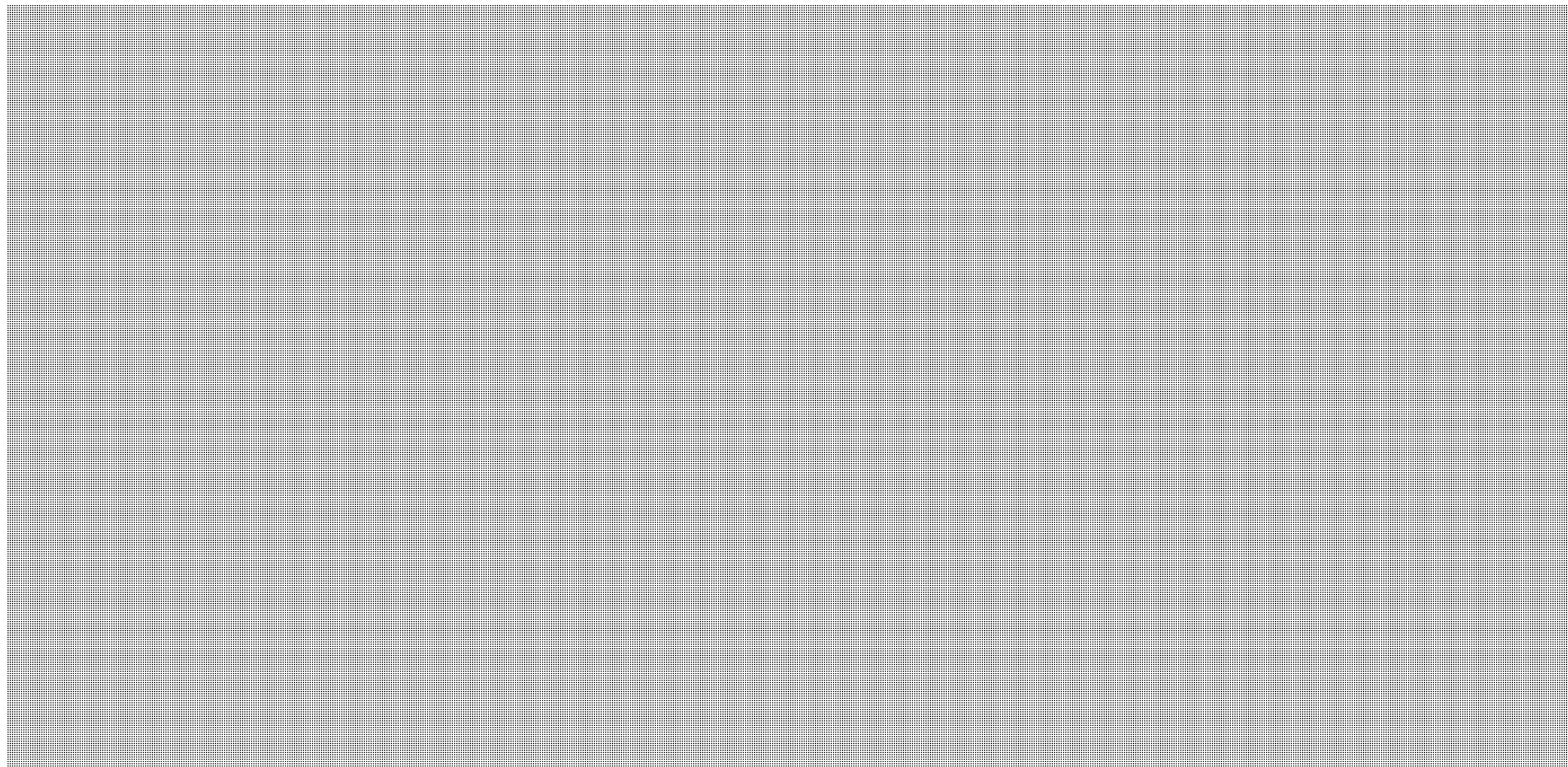
From: [REDACTED]
Sent: October 4, 2011 11:06 AM
To: Beaudoin, Luc S, [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential

Yes,

Luc, are you or your team available to have a discussion on this and if so when?

Regards,

s.16(2)(c)



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.



Pages 167 to / à 171
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

s.20(1)(c)

Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 19, 2011 4:47 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

PROTECTED

Limited Distribution

[REDACTED] is one we know has an API with [REDACTED] and seems to display this issue. But again, these are merchant-side apps and may not be used at all by [REDACTED]. Most likely, the team looking at on-line services / eCommerce for [REDACTED] would have an idea of the API concerned. The concern is that potentially private information like credit card data be exchanged in the clear where the user expects it to be SSL all the way.

thanks alot again...

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]
Sent: September 19, 2011 4:24 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

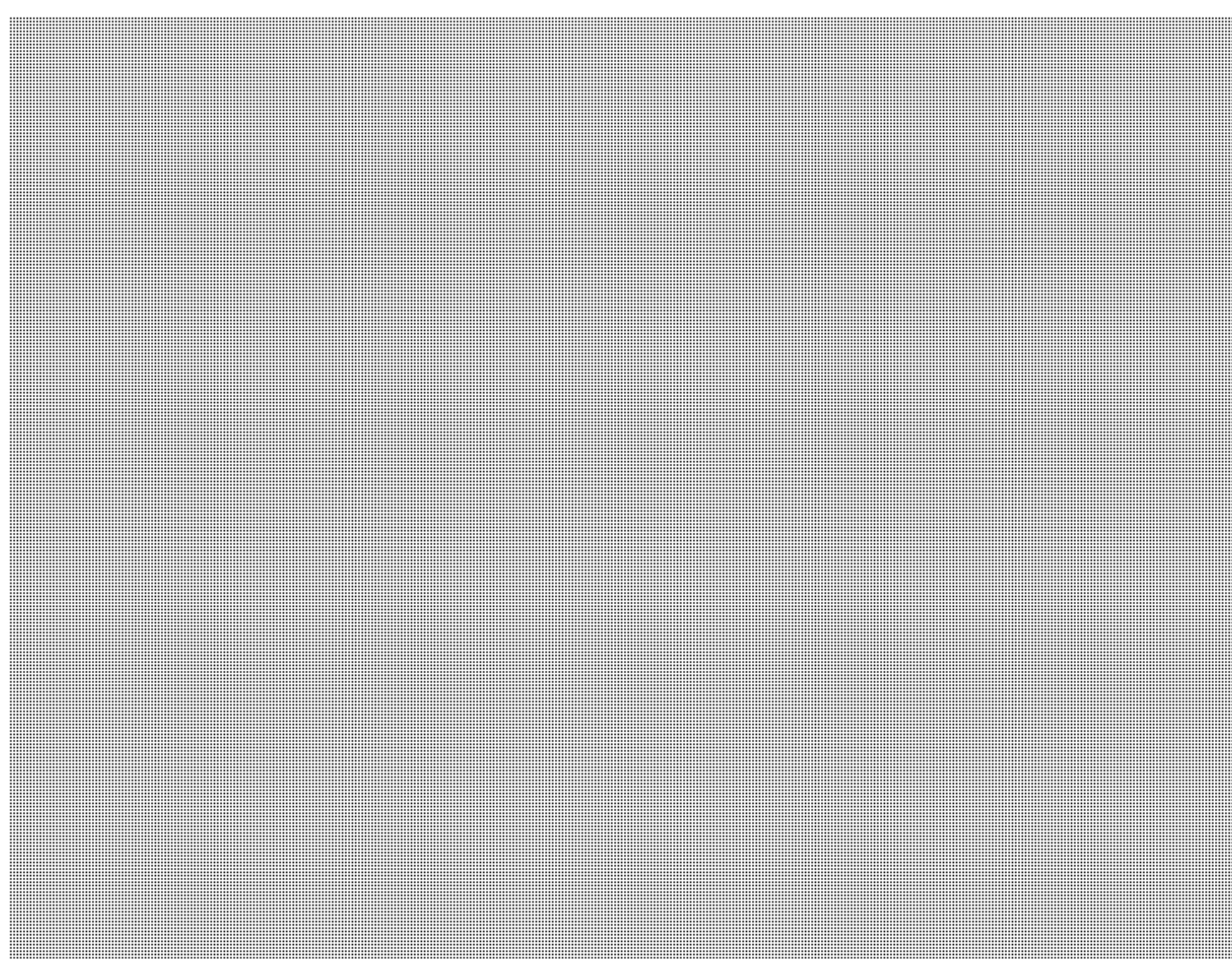
Hi Luc,

I am still trying to get information on this issue. Do you have a particular app/web you can point to?

Regards,

s.16(2)(c)

s.20(1)(c)



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 16, 2011 11:39 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

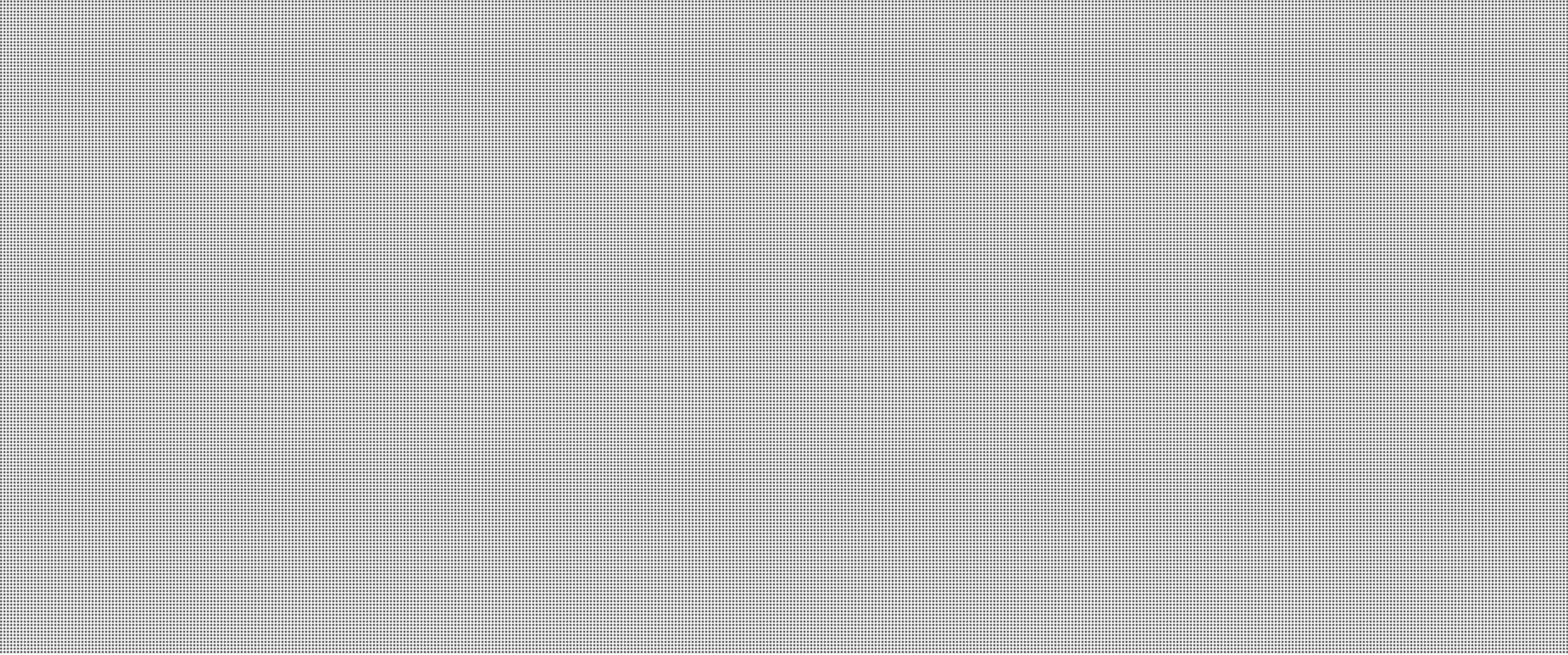
PROTECTED

Limited Distribution (within Need to Know Technical Staff of your organisation)

The issue is reported in PHP implementation of cURL options for certificate check in SSL transaction between 2 servers (generally between merchant and transaction processor) . Specifically, a software package called [REDACTED] amongst others, implements a [REDACTED] API which seems to be affected. Here are some details:

CURLOPT_SSL_VERIFYPEER seems turned off in [REDACTED]
[REDACTED]

Module:



s.16(2)(c)

s.20(1)(c)

Question:

- What would these API be used for ?
- Do you know how prevalent is [REDACTED] amongst your merchants ?
- Do you know if [REDACTED] expects merchant applications to properly authenticate SSL connections ?

thanks for your help

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

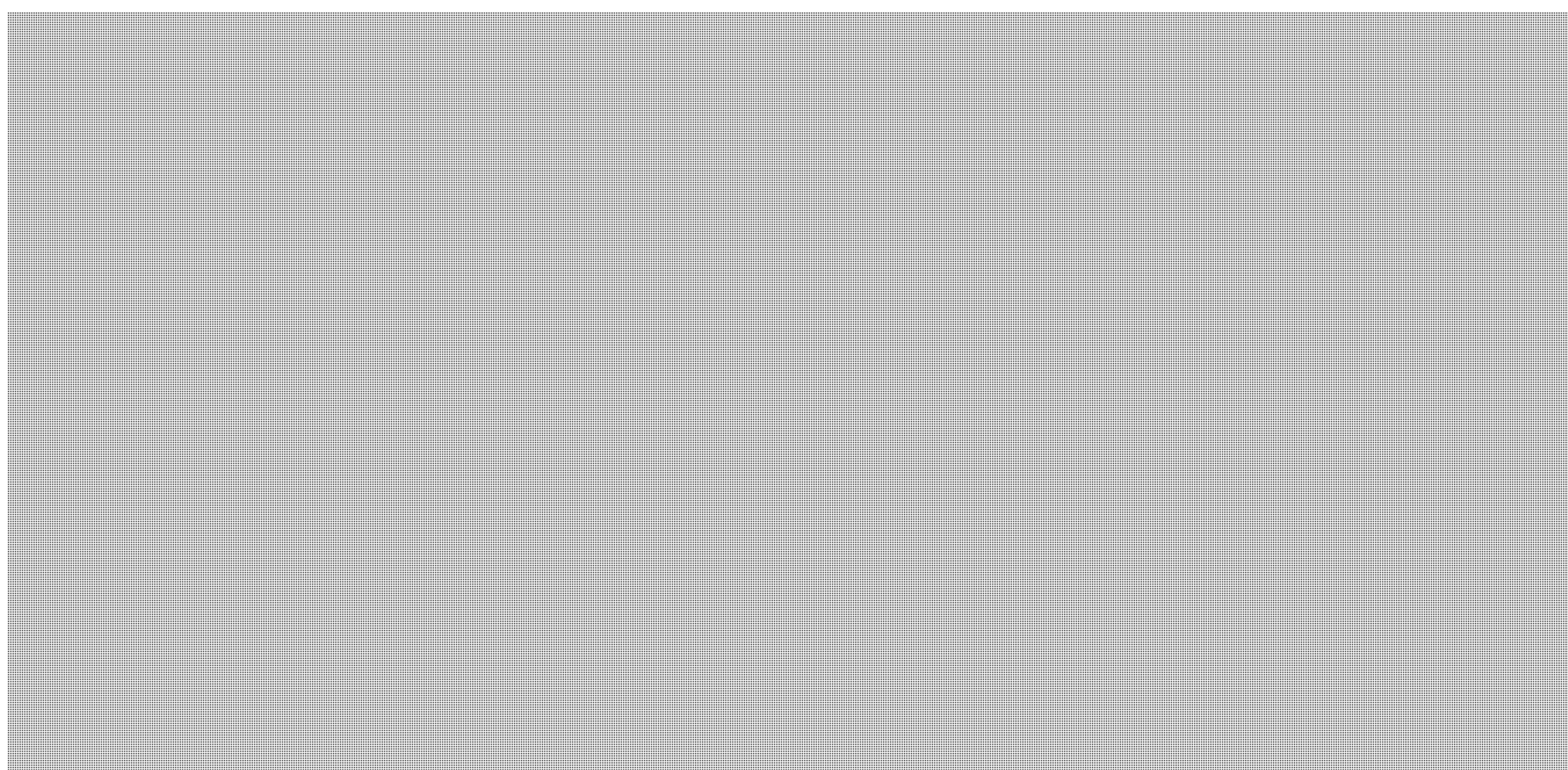
s.16(2)(c)

From: [REDACTED]
Sent: September 16, 2011 10:44 AM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

Hi Luc,

As per my voice mail, would it be possible to send more detail as to the particular app?

Regards,



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 15, 2011 5:25 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: AC2971 contact for PHP based ecommerce site

I am trying to locate someone in [REDACTED] who might be involved with the online store applications used to process on-line payments by affiliated merchants. I beleive there is an API the group uses which leverages PHP cURL and certificate options for which we are researching a potential vulnerability/configuration issue.

any help would be great.

cheers

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

s.16(2)(c)

s.20(1)(c)

Breault, Stephen

From: Beaudoin, Luc S
Sent: Tuesday, October 04, 2011 2:58 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

Sensitivity: Confidential

Mark sent me some info on this already. Thanks !

[REDACTED] software company for ecommerce applications

cheers

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]
Sent: October 4, 2011 2:51 PM
To: Beaudoin, Luc S [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential

Hi Luc,

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: October 4, 2011 11:50 AM
To: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential

s.16(2)(c)

s.20(1)(c)

reviewing the email chain, we may not need to have a teleconference. Would you guys happen to have a trusted contact with [REDACTED] we could use to discuss this issue with them ?

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]
Sent: October 4, 2011 11:06 AM
To: Beaudoin, Luc S; [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Sensitivity: Confidential

Yes,
Luc, are you or your team available to have a discussion on this and if so when?

Regards,

s.16(2)(c)

s.20(1)(c)

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

Pages 181 to / à 183
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c)

of the Access to Information
de la Loi sur l'accès à l'information

s.20(1)(c)

Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 19, 2011 4:47 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

PROTECTED
Limited Distribution

[REDACTED] one we know has an API with [REDACTED] seems to display this issue. But again, these are merchant-side apps and may not be used at all by [REDACTED]. Most likely, the team looking at on-line services / eCommerce for [REDACTED] would have an idea of the API concerned. The concern is that potentially private information like credit card data be exchanged in the clear where the user expects it to be SSL all the way.

thanks alot again...

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

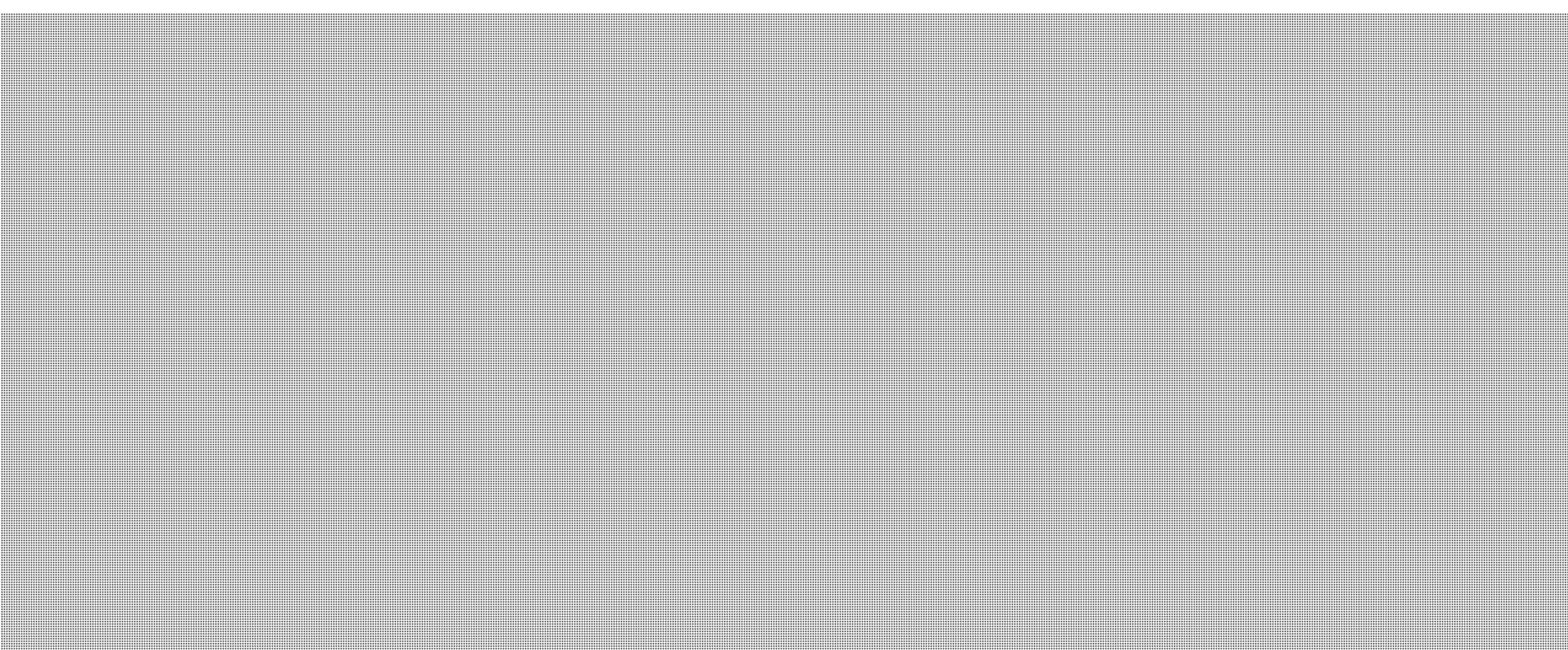
<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]
Sent: September 19, 2011 4:24 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site
Hi Luc,

s.20(1)(c)

I am still trying to get information on this issue. Do you have a particular app/web you can point to?

Regards,



Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

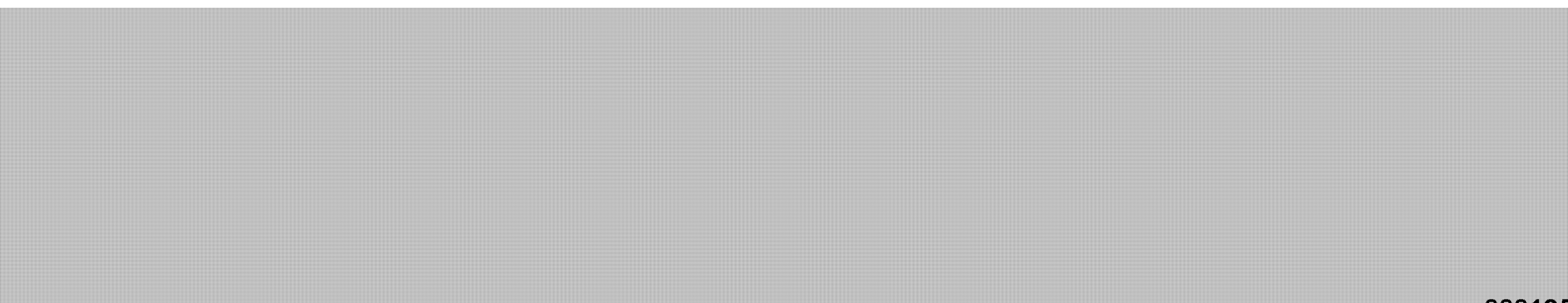
L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: September 16, 2011 11:39 AM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: AC2971 contact for PHP based ecommerce site

PROTECTED

Limited Distribution (within Need to Know Technical Staff of your organisation)

The issue is reported in PHP implementation of cURL options for certificate check in SSL transaction between 2 servers (generally between merchant and transaction processor) . Specifically, a software package called Prestashop, amongst others, implements a CanadaPost API which seems to be affected. Here are some details:



s.16(2)(c)

s.20(1)(c)

Question:

- What would these API be used for ?
- Do you know how prevalent is [REDACTED] amongst your merchants ?
- Do you know if [REDACTED] expects merchant applications to properly authenticate SSL connections ?

thanks for your help

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

From: [REDACTED]

Sent: September 16, 2011 10:44 AM

To: Beaudoin, Luc S

Cc: [REDACTED]

Subject: RE: AC2971 contact for PHP based ecommerce site

Hi Luc,

As per my voice mail, would it be possible to send more detail as to the particular app?

Regards,

[REDACTED]

Security - Everyone's Responsibility/La Sécurité – chacun en est responsable!

The information contained in this communication and its attachment(s) is intended solely for the individual to whom it is addressed. It may contain protected, privileged or confidential information. Any unauthorized disclosure, distribution or copying is strictly prohibited. If you have received this message in error, please notify us immediately and delete the original message. Thank you.

L'information contenue dans cette communication et les pièces qui y sont jointes vise uniquement la personne à qui elle s'adresse. Il peut s'agir de renseignements protégés, privilégiés ou confidentiels. Il est strictement interdit de divulguer, de distribuer ou de copier l'information sans autorisation préalable. Si vous avez reçu ce message par erreur, veuillez communiquer immédiatement avec nous et supprimer le message original. Merci.

s.16(2)(c)

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]

Sent: September 15, 2011 5:25 PM

To: [REDACTED]

Cc: [REDACTED]

Subject: AC2971 contact for PHP based ecommerce site

Hi [REDACTED]

I am trying to locate someone in [REDACTED] who might be involved with the online store applications used to process on-line payments by affiliated merchants. I believe there is an API the group uses which leverages PHP cURL and certificate options for which we are researching a potential vulnerability/configuration issue.

any help would be great.

cheers

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

<<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf> <<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>>

s.16(2)(c)

s.19(1)

s.20(1)(c)

Breault, Stephen

From: Beaudoin, Luc S
Sent: Wednesday, October 05, 2011 11:01 AM
To: [REDACTED]
Subject: RE: 2971: Notification [REDACTED] potential security issue

Yes, it is under Activity 2971 [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----

From: [REDACTED]
Sent: October 5, 2011 10:19 AM
To: Beaudoin, Luc S
Subject: FW: 2971: Notification [REDACTED] potential security issue
Importance: High

Has an activity or event been created for this? I can't find any other references to it.

Thanks,

Julia Scouten CISSP GCIA GCIH GSEC
Incident Handler
Canadian Cyber Incident Response Centre (CCIRC) Public Safety Canada Julia.Scouten@ps-sp.gc.ca 613-991-7070

-----Original Message-----

From: [REDACTED]
Sent: October 4, 2011 4:49 PM
To: [REDACTED]
Subject: Re: 2971: Notification [REDACTED] potential security issue
Importance: High

Luc,

I have the proper key and have decrypted the message. We are reviewing the issue now. Thank you for your submission.

On 10/3/11 11:32 AM, '[REDACTED]' wrote:

>Thanks for the quick reply. Find details attached [REDACTED]

[REDACTED] We would appreciate your thoughts on this.

>

>Cheers

>

>Luc Beaudoin, P.Eng, MSc, MBA

s.16(2)(c)

>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

s.19(1)

>Cyber Incident Response Centre | Centre canadien de réponse aux

s.20(1)(c)

>incidents cybernétiques Public Safety Canada | Sécurité publique Canada

>Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1

>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of

>Canada | Gouvernement du Canada

>

>

>Need to report an incident? Find the Incident Report Form here:

>

>

><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/it>

>imp

>-pgimti-app-ann-D-eng.rtf

>

>Vous voulez rapporter un incident ? Utilisez le formulaire de

>déclaration

>suivant:

>

><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/it>

>imp

>-pgimti-app-ann-D-fra.rtf

>

>

>

>

>-----Original Message-----

>From [REDACTED]

>Sent: October 3, 2011 12:22 PM

>To: [REDACTED]

>Subject: Re: 2971: Notification [REDACTED] potential security issue

>Importance: High

>

>Luc,

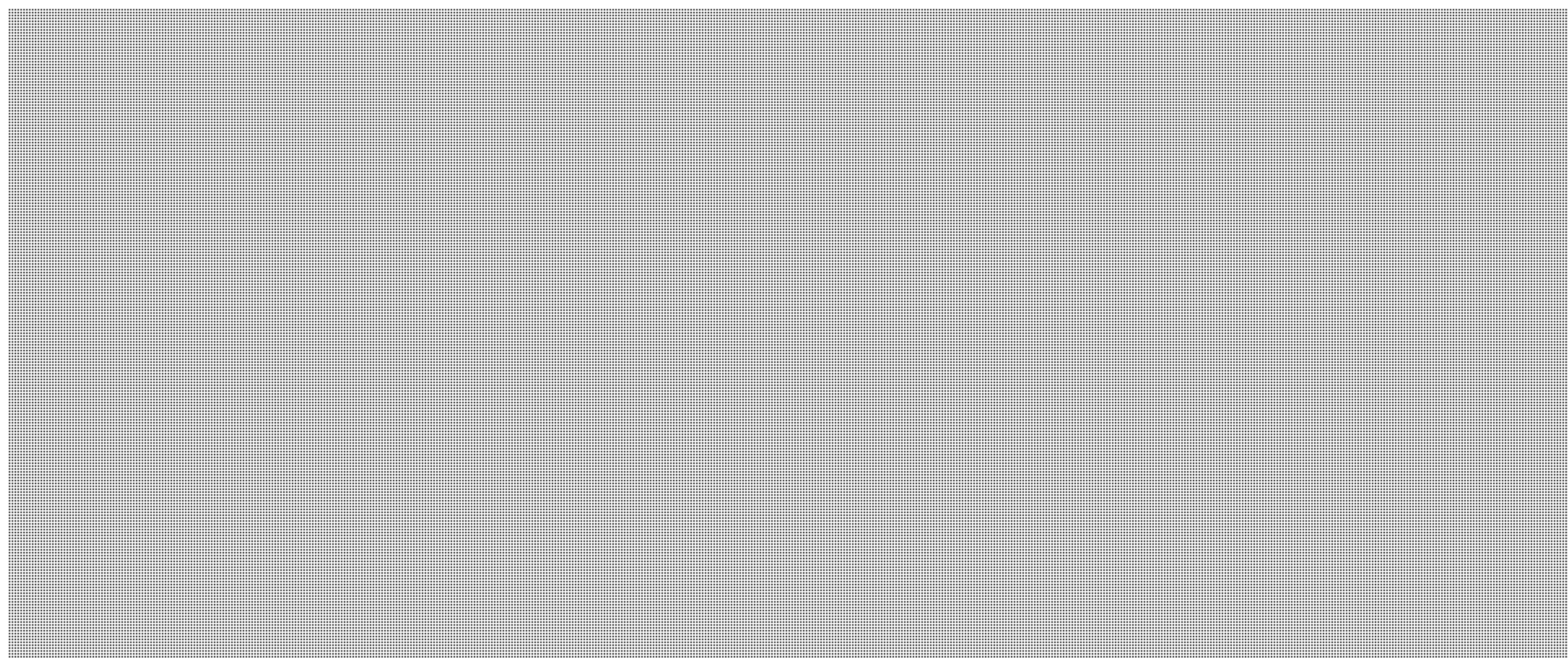
>

>I am a member of the Security Operations Center at [REDACTED] Please

>provide more information in regards to your discovery. Thanks.

>

>



>

>

>
>thank you
>
>Luc Beaudoin, P.Eng, MSc, MBA
>Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>Cyber Incident Response Centre | Centre canadien de réponse aux
>incidents cybernétiques Public Safety Canada | Sécurité publique Canada
>Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1
>613-991-3574 luc.beaudoin@ps-sp.gc.ca<<mailto:luc.beaudoin@ps-sp.gc.ca>>
>PublicSafety.gc.ca
>Government of Canada | Gouvernement du Canada
>
>
>Need to report an incident? Find the Incident Report Form here:
>
>
><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>
>imp
>-pgimti-app-ann-D-eng.rtf
>
>Vous voulez rapporter un incident ? Utilisez le formulaire de
>déclaration
>suivant:
>
><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>
>imp
>-pgimti-app-ann-D-fra.rtf<[http://www.tbs-sct.gc.ca/sim-gsi/publications](http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf)
>/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>
>
>

Breault, Stephen

From: [REDACTED]
Sent: Thursday, October 20, 2011 1:05 PM
To: Beaudoin, Luc S; [REDACTED]
Subject: RE: Peer Hijacking

s.16(2)(c)

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Thursday, October 20, 2011 3:58 PM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: Re: Call this morning?

On 11-10-19 02:04 PM, Beaudoin, Luc S wrote:

> Thanks very much Kevin. Here is another draft with some of the comments integrated. I would like to keep the product as generic as possible to avoid the trap of tracking every possible implementations and versions (which could be legitimately requested by any of these software companies). Not sure however if this will be possible by listing the products like we do at the moment.

>

> The table is a good idea if in the end we want to track versions, and more importantly, download page for non-vulnerable updates.

>

> As for cURL, I am pretty sure about the acronym:

> <http://php.net/manual/en/book.curl.php>

>

> For discussion tomorrow.

>

> cheers

>

> Luc Beaudoin, P.Eng, MSc, MBA

> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

> Cyber Incident Response Centre | Centre canadien de réponse aux

> incidents cybernétiques Public Safety Canada | Sécurité publique

> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur

> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government

> of Canada | Gouvernement du Canada

>

>

>

> -----Original Message-----

> From: [REDACTED]

> Sent: October 13, 2011 5:10 PM

> To: Beaudoin, Luc S

> Cc: [REDACTED]

> Subject: Re: Call this morning?

>

[REDACTED]

s.19(1)

>
> On 11-10-13 09:17 AM, Beaudoin, Luc S wrote:
>> //////////////////////////////////
>>
>>
>> La version française suit
>>
>>
>> PUBLIC SAFETY CANADA
>> CANADIAN CYBER INCIDENT RESPONSE CENTRE
>>
>> *****
>> INFORMATION NOTE
>> *****
>>
>> Number: IN11-XXX
>> Date:
>>
>> *****
>> IMPLEMENTATING PHP CURL VERIFYPEER OPTION IN APPLICATIONS REQUIRING SSL CERTIFICATE VERIFICATION
>> *****
>>
>>
>> PURPOSE
>> =====
>>
>> The goal of this advisory is to raise awareness of a common but potentially insecure implementation of the PHP cURL
option used to verify SSL certificates.
>>
>>
>> ASSESSMENT
>> =====
>>
>> The PHP Hypertext Processor (PHP) is a flexible server-side scripting language and environment. It allows developers
to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (cURL
or libcurl). The cURL library regroups a set of functions which allow establishing connections using various
communication protocols including http, https, ftp, gopher, telnet, dict, file, and ldap. This PHP library can also be used
to implement security features such as HTTPS certificates, proxies, cookies and user-password authentication. As a
result, the cURL library is commonly used by web application developers, particularly in eCommerce applications, to
establish connections between system components hosted on different network segments, such as payment processing
service APIs.
>>
>> The cURL curl_setopt function allows for setting a number of options, including the verification of SSL certificates
against relevant Certificate Authorities or predefined certificates store bundled with the web application. The option
called CURLOPT_SSL_VERIFYPEER, which is set to a value of "1", or "true", by default (from cURL 7.10), enforces the
verification of the signing authority for peer certificates presented prior to establishing the SSL connection.

Unfortunately, this option is often overridden to "0", or "false", which disables the certificate verification process. This may allow for any self-signed peer certificates to be trusted. As cURL functions are generally used for server to server connections, the owner of the information and the operator of the application server, such as the merchant in an eCommerce application case, may therefore be unaware should an untrusted certificate be presented to establish a connection instead of a valid one. This could be the case for different variants of man-in-the-middle attacks.

>>

>>

>>

>> The way the cURL library verifies that a peer Certificate is valid is by using of a list of trusted Certificate Authorities (CA) referred to as ca-bundle. This list must have its path referenced accordingly by the developer using the CURLOPT_CAINFO option (pointing to a .crt or .pem file). Alternatively, the developer may point to a specific certificate directory to be used for verification using the CURLOPT_CAPATH option.

>>

>> For implementations details, developers may refer to the following guidance:

>>

>>

>> SUGGESTED ACTION

>> =====

>>

>> CCIRC recommends that operator of web applications which implement TLS/SSL connections using the PHP cURL library, verify that the CURLOPT_SSL_VERIFYPEER option is set to True, or "1", and that failure to return a successful verification results in a failed connection error rather than establishing an untrusted or insecure connection. Searching application code directory for the entries similar as the following will provide indications of the settings used in your cURL implementation:

>> Examples:

>> curl_setopt(\$connection, CURLOPT_SSL_VERIFYPEER, 1);

>> curl_setopt(\$connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");

>> curl_setopt(\$connection, CURLOPT_CAINFO, "path:/ca.pem");

>> Specifically the strings "CURLOPT_SSL_VERIFYPEER" and "CURLOPT_CAINFO" .

>>

>>

>> CCIRC recommends that transaction processing organisation review and ensures their PHP API enforces proper implementation of certificate verification by affiliated merchants and partners.

>>

>> //////////////////////////////////

>>

>>

>> Luc Beaudoin, P.Eng, MSc, MBA

>> Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>> Cyber Incident Response Centre | Centre canadien de réponse aux
>> incidents cybernétiques Public Safety Canada | Sécurité publique
>> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur
>> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
>> +Government
>> of Canada | Gouvernement du Canada

s.16(2)(c)

s.19(1)

>>
>>
>>

>> -----Original Message-----

>> From: Beaudoin, Luc S

>> Sent: October 13, 2011 12:11 PM

>> To: [REDACTED]

>> Cc: [REDACTED]

>> Subject: RE: Call this morning?

>>

>> [REDACTED]

>>

>>

>> Luc Beaudoin, P.Eng, MSc, MBA

>> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>> Cyber Incident Response Centre | Centre canadien de réponse aux

>> incidents cybernétiques Public Safety Canada | Sécurité publique

>> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur

>> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca

>> +Government

>> of Canada | Gouvernement du Canada

>>

>>

>>

>> -----Original Message-----

>> From: [REDACTED]

>> Sent: October 13, 2011 12:12 PM

>> To: Beaudoin, Luc S

>> Cc: [REDACTED]

>> Subject: Re: Call this morning?

>>

>> [REDACTED]

>>

>> --

>>

>> [REDACTED]

>>

>> On 11-10-13 09:09 AM, Beaudoin, Luc S wrote:

>>> Catching up. I am waiting on the call. I was 5 minutes late.

>>>

>>> Luc

>>>

>>>

>>> Luc Beaudoin, P.Eng, MSc, MBA

>>> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

s.19(1)

>>> Cyber Incident Response Centre | Centre canadien de réponse aux
>>> incidents cybernétiques Public Safety Canada | Sécurité publique
>>> Canada Telephone | Téléphone +1 613-991-9949 Facsimile |
>>> Télécopieur
>>> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
>>> +Government
>>> of Canada | Gouvernement du Canada
>>>
>>>
>>>
>>> -----Original Message-----
>>> From: [REDACTED]
>>> Sent: October 13, 2011 11:04 AM
>>> To: [REDACTED] Beaudoin, Luc S
>>> Subject: Call this morning?
>>>
>>> [REDACTED]
>>> [REDACTED]
>>> --
>>>
>> [REDACTED]

s.16(2)(c)

s.19(1)

s.20(1)(e)

Breault, Stephen

From: Beaudoin, Luc S
Sent: Tuesday, October 25, 2011 2:57 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: CCIRC Activity 2971: [REDACTED]
Attachments: [REDACTED]

Good afternoon [REDACTED]

as discussed, I would appreciate your feedback on this proposed product regarding the issue brought up over the summer. Specifically, I would appreciate if you could comment on the issue of listing some of the potentially affected software so that developers and merchants/users can review their current installations and take appropriate actions. Typically, such a product would include a URL to software manufacturer for users to download the latest version of the software.

I have removed the other [REDACTED] software potentially affected [REDACTED] and we will do the same with yours in others' notification.

Once finalized, this product would be posted on the PS CCIRC website here:

<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

[REDACTED]
[REDACTED] The target is 1 Nov, and this is largely due to the fact that some other affected software are open source projects for which it will be difficult to limit the availability of the information once notified.

Thanks

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Breault, Stephen

From: Beaudoin, Luc S
Sent: Wednesday, October 26, 2011 2:59 PM s.16(2)(c)
To: [REDACTED] s.19(1)
Subject: Potential Security Issue affecting [REDACTED] s.20(1)(c)
Importance: High

Good day,

Could you assist us with identifying the best mechanism/contact to bring forward a potential security issue in [REDACTED] code ?

Thank you

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

s.19(1)

Breault, Stephen

From: Luc Beaudoin [REDACTED]
Sent: Wednesday, October 26, 2011 6:45 PM
To: Beaudoin, Luc S
Subject: ecommerce patching

register

Marcus Carey, security researcher & community manager at Rapid7, said that outsourcing practices had exacerbated the patching deficiencies that the worm exploited.

"Many businesses outsource web application development and once the application is deployed, service contracts may lapse or IT staff may not be paying much attention to them," Carey said.

"The use of this new malware associated with JBoss is something we have not seen before. However, the actual vulnerability it is exploiting should have been snuffed out years ago. This is far more a business failure than a software security failure at this point," he added.

s.16(2)(c)

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Wednesday, October 26, 2011 3:35 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]

[REDACTED]

On 11-10-26 12:27 PM, Beaudoin, Luc S wrote:

s.16(2)(c)

s.19(1)

cat and mouse. They want to make sure we checked it first....

s.20(1)(c)

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

From: [REDACTED]

Sent: October 26, 2011 3:27 PM

To: Beaudoin, Luc S

Subject: Re: [REDACTED]

On 11-10-26 12:23 PM, Beaudoin, Luc S wrote:

Quick one:

which version did you review ? Was it the latest [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Breault, Stephen

From: Beaudoin, Luc S
Sent: Wednesday, October 26, 2011 9:55 PM
To: [REDACTED]
Subject: Re: [REDACTED] potential security issue

Indeed, this is the issue. We are trying to notify all these groups and some have committed to updates already [REDACTED]. This is a m-i-m exposure, and as you know, if there is a m-i-m between an ecommerce site and a transaction processing service, there are a few problems on top of this one. But we think this may not chain properly the trust a user expects when connecting by browser with an ecommerce application over a properly authenticated SSL session to have the same site pass-on the information at a lower security level.

Once [REDACTED] updated its code, would you be in a position to update yours accordingly and notify your community to update ?

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [REDACTED]
Sent: Wednesday, October 26, 2011 05:07 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED] potential security issue

Hey Luc:

[REDACTED]

```
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);  
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
```

(just downloaded this a few mins ago from:

[REDACTED]

the link:

[REDACTED]

Do you think this issue should be addressed at that level [REDACTED] we definitely want to adhere to best practices.

[REDACTED]

What are your thoughts? and how big a security hole is it ? (and if so, any idea [REDACTED] it set to false)

Also [REDACTED] sets it to false. [REDACTED] has it conditionally set to true with a comment of set to false if having connection problems

s.16(2)(c)

lobo

s.20(1)(c)

On 10/26/11 3:44 PM, Beaudoin, Luc S wrote:

The code appears to still have some PHP files with the cURL VERIFYPEER option set to False. This setting may prevent the proper validation of the SSL certificate and make the application connection to the information processing service unsecured or vulnerable to self-signed certificates and man-in-the-middle attacks.

[REDACTED]

We would like to raise awareness of this coding practice amongst key ecommerce package development communities to avoid server-to-server communications being potentially vulnerable.

We have specifics on other modules this may affect, but I would like to know if you were aware of this potential issue and what your thoughts may be about its significance.

thanks

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

s.16(2)(c)

s.19(1)

s.20(1)(c)

From: Beaudoin, Luc S
Sent: October 26, 2011 3:20 PM
To: [REDACTED]
Subject: RE: [REDACTED] potential security issue

We will. thanks. The issue had to do with the default setting of the PHP cURL VERIFYPEER option in various payment modules. This option appears to be set to false, which could result in unvalidated SSL connections.

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: October 26, 2011 3:03 PM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]

[REDACTED]
can you please ensure that the security issue is on the latest version of the [REDACTED]

thanx
[REDACTED]

On 10/26/11 2:24 PM, Beaudoin, Luc S wrote:

Good day,

Could you provide us with a contact/mechanism to communicate a potential security issue reported to us potentially affecting [REDACTED]

thanks

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Breault, Stephen

From: Beaudoin, Luc S
Sent: Thursday, October 27, 2011 11:23 AM
To: [REDACTED]
Subject: RE: [REDACTED] potential security issue
Attachments: [REDACTED] version.txt

I think you are right in that it was probably disabled for testing purposes and simplicity sake. Defaulting to a secure configuration, with notes in the code explaining that if disabled for testing to not forget to re-enable afterwards would be a sound approach. Note also that PCI latest norms underline the importance of properly validating end-points.

We are looking at publishing the attached product in the upcoming days/weeks. We could synchronize release with your update and add a reference to it. I would appreciate your thoughts on this proposal.

The link to where this product would be posted is: <http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>
<<http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>>

L

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: October 27, 2011 7:55 AM
To: Beaudoin, Luc S
Subject: Re: [REDACTED]

We are going into a code freeze for the next version in 2 weeks? Is it ok for this fix to be in the [REDACTED]? We'll need to make it a setting so that users can turn it off when connecting to sandbox sites for testing purposes

[REDACTED]

On 10/26/11 9:54 PM, Beaudoin, Luc S wrote:

Indeed, this is the issue. We are trying to notify all these groups and some have committed to updates already [REDACTED] This is a m-i-m exposure, and as you know, if there is a m-i-m between an ecommerce site and a transaction processing service, there are a few problems on top of this one. But we think this may not chain properly the trust a user expects when connecting by browser with an ecommerce application over a properly authenticated SSL session to have the same site pass-on the information at a lower security level.

[REDACTED] its code, would you be in a position to update yours accordingly and notify your community to update ?

Luc Beaudoin

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

s.16(2)(c)

From: [REDACTED]

s.19(1)

Sent: Wednesday, October 26, 2011 05:07 PM

s.20(1)(c)

To: Beaudoin, Luc S

Subject: Re: [REDACTED] potential security issue

Hey Luc:

We copied that code from [REDACTED]

(just downloaded this a few mins ago from:

[REDACTED]
the link:

[REDACTED]

Do you think this issue should be addressed at that level? From a [REDACTED] we definitely want to adhere to best practices.

[REDACTED]

What are your thoughts? and how big a security hole is it ? (and if so, [REDACTED] still wants it set to false)

Breault, Stephen

From: [REDACTED]
Sent: Friday, November 04, 2011 1:25 PM
To: [REDACTED]
Subject: RE: CANCELLATION today's teleconf...POSTPONE to tomorrow ?



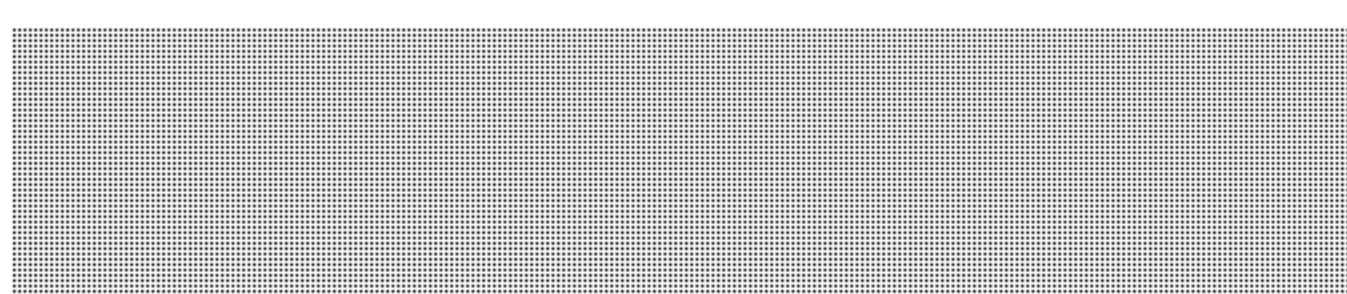
s.16(2)(c)

s.19(1)

s.20(1)(c)

From: [REDACTED]
Sent: November 4, 2011 1:16 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: CANCELLATION today's teleconf...POSTPONE to tomorrow ?

OK, so I missed the call. My deepest apologies. Do we need another time early next week or just touch base next Thursday ? I have the following update:



Breault, Stephen

From: Beaudoin, Luc S
Sent: Friday, November 04, 2011 2:31 PM
To: [REDACTED]
Subject: RE: CANCELLATION today's teleconf...POSTPONE to tomorrow ?

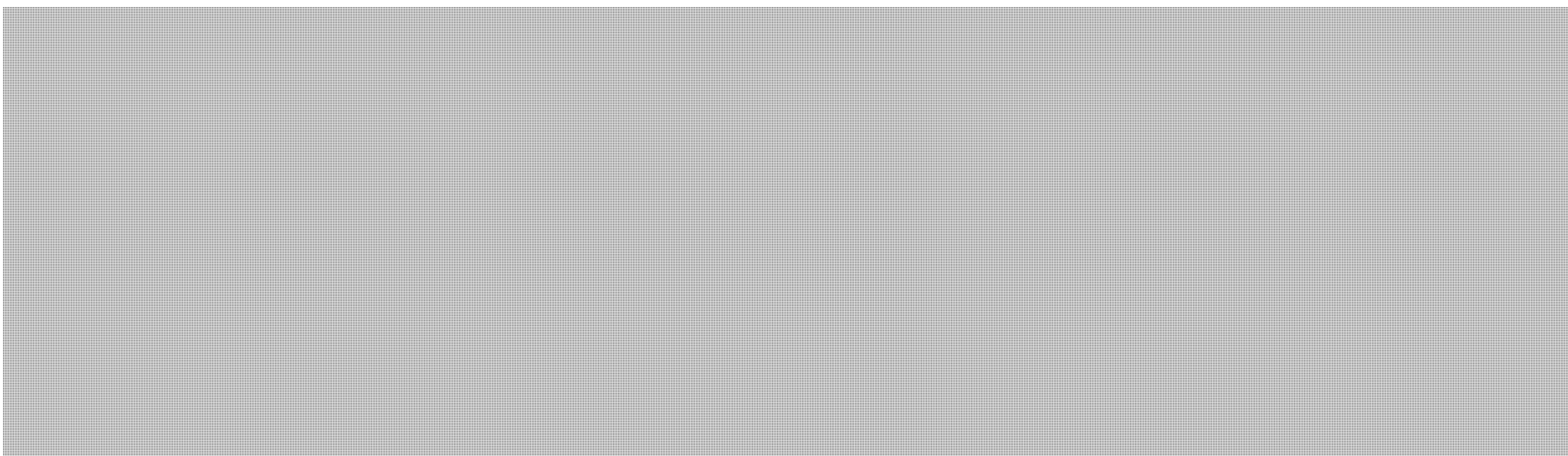
activity 2971, in July

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: November 4, 2011 2:30 PM
To: Beaudoin, Luc S
Subject: FW: CANCELLATION today's teleconf...POSTPONE to tomorrow ?

Where can I file these emails? Is there an event / activity open?

From: [REDACTED]
Sent: Friday, November 04, 2011 2:29 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: CANCELLATION today's teleconf...POSTPONE to tomorrow ?



--

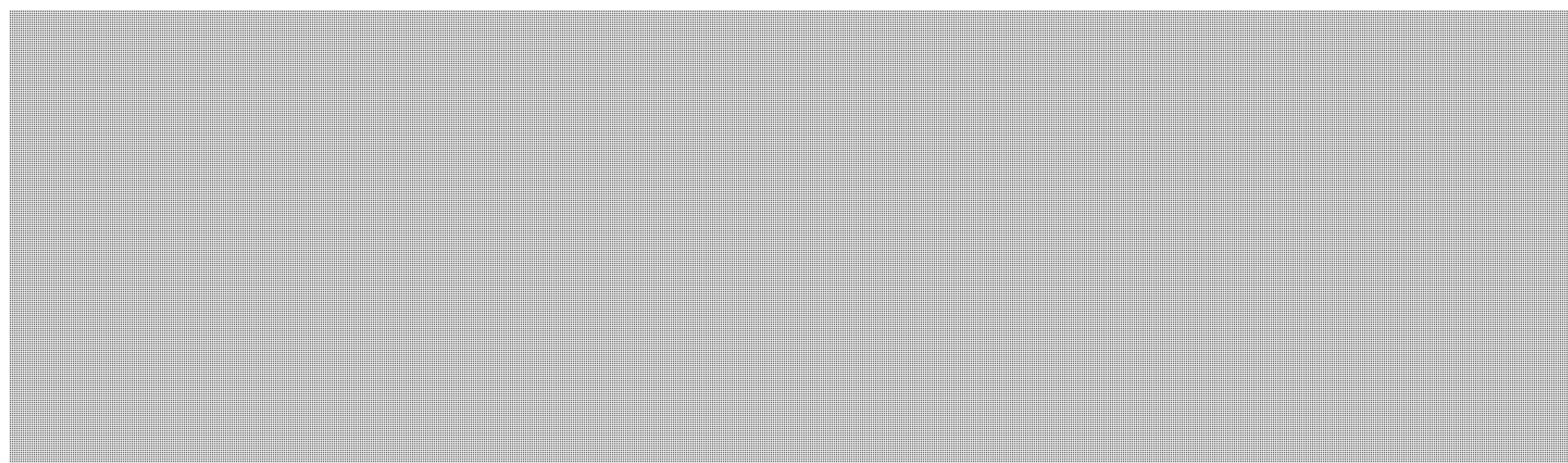
s.16(2)(c)

s.19(1)

s.20(1)(c)

On 11-11-04 10:15 AM, [REDACTED] wrote:

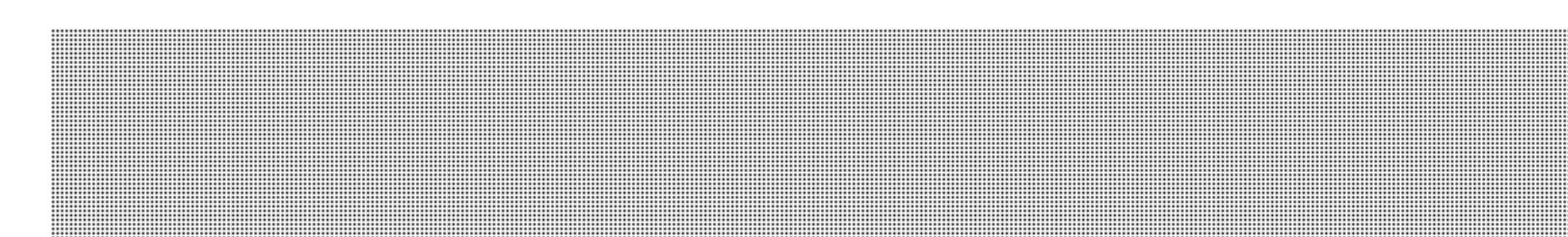
OK, so I missed the call. My deepest apologies. Do we need another time early next week or just touch base next Thursday ? I have the following update:



Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: November 3, 2011 12:06 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: CANCELLATION today's teleconf...POSTPONE to tomorrow ?



On 11-11-03 06:54 AM, [REDACTED] wrote:

From: [REDACTED]
Sent: November 3, 2011 9:47 AM
To: [REDACTED]
Subject: CANCELLATION today's teleconf...POSTPONE to tomorrow ?

Gentlemen, would you mind postponing our weekly teleconference to tomorrow, Friday, 12h ? I cannot make today's timing....

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: October 27, 2011 3:07 PM
To: [REDACTED]
Subject: RE: pci

From: [REDACTED]
Sent: October 27, 2011 12:50 PM
To: [REDACTED]
Subject: RE: pci

<http://www.fcac-acfc.gc.ca/> <<http://www.fcac-acfc.gc.ca/>>

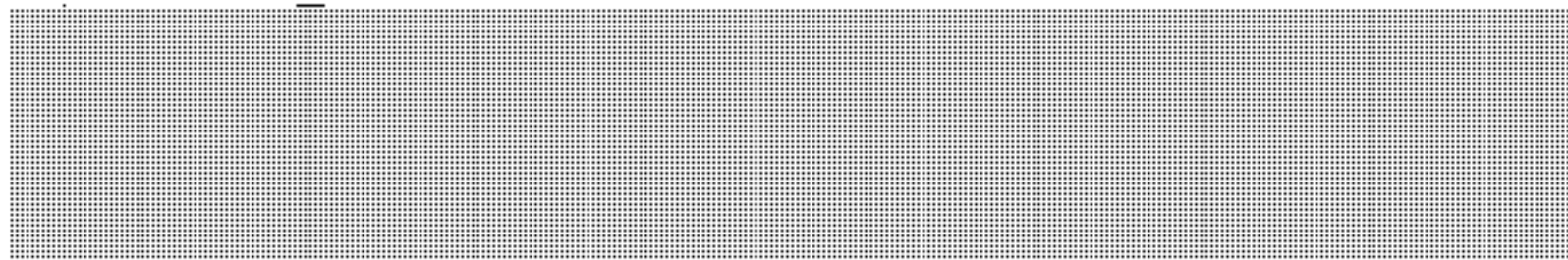
Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <<mailto:luc.beaudoin@ps-sp.gc.ca>>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

s.19(1)

From: [REDACTED]
Sent: October 27, 2011 12:45 PM
To: Beaudoin, Luc S; [REDACTED]
Subject: pci

[REDACTED]

Breault, Stephen

From:	Beaudoin, Luc S	
Sent:	Tuesday, November 15, 2011 10:48 PM	
To:		s.16(1)(b)
Cc:		s.16(2)(c)
Subject:	PHP cURL use in eCommerce packages	

-----BEGIN PGP MESSAGE-----

Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

qANQR1DBwEwDTamhORmi/ZABCACt5uzhvDVyd5MagnAcV7/I5SkLod5OyRk0Zoig
P0286U3lv9/QWGDHD3B4dMmklg5r1RRh5FstCOcd2m61p9eiya5aVl4tOS1nu5d
IJN+2n94pX5m31EMvu7PVM12Gp4HaVBAWQv5nng8W6c83WO1tgeGtH+HyrPfLpz4
ZjOU1lsUB3dBD53lX0otuGvSqNkM0GGaPwMBRC7iva4AbnJLvHQEYVal3elD1j7B
TbsDMRAD8+yXw2EwW2shnw59UYwJWjjW6og8X2dXLBpZrMpsmpqrBLdtgKgFAw9S
9OwB9M3uYrvhalWEIRb/qUCd0RlThV3mlPpaJwD7px/3NzqxwcBMA02tpa/PqTbo
AQf/QfLI8NS0vFeXo+Uzx5lGMYesDzjQTHw2MJdwTyl2l5slNBxB88/053Tx0yW
4WwHWGDwlhc6oYzid6OuLuHyqvGZyGjQOA1Qpye8yVeEw8xOk7rstkF3+DLmn8d
OFCuuDLN7khDmsplRQ3qOp0Xe09G+SpqKFB6Jd5KrG15rEfuUjHp9vPQLPZkAcLK
vjmERu5ZMRPBFVoe7a74/xeClE6ktjNGn2VGCEK0UqrL3nLjY5RfYEM+AlkUgSLX
1430rA1mVYgXElcrGiZFx1n0BrCKc3ol4PtgiBF3sU0Y/9D5lqWl0udcsmx4DK5U
pBO7JyX5YCXdyF/Yv/sgUOBBJ8HBTgOL+y6OUJhtoRAH/inBbxod4Ljo7ix4yLkM
EwyV7vezy5/MnpVBAR3pn3Blp2npg6UM77VMVRR4TW7wNt+easIMwfZzd8z+KxkZ
NKp8tgCsZVlq7NxFS5aBfScE5eTP1GGGxgiAWjR9QxjHOY+Ln27JeRFczmq6osBV
632+9grXZSMFbxon0gYLkP+qDiKpsl0YsWvWgF1x2VgqSiCzf63PhAm628ppDn09
ANlb+S9+JYBPn94mXJSyt4GomsKQEGFDaeiwd38MdWFLs2roX/Me3SsSIAdih0bP
K1utZFGKummBlr/iaSOvaQc2A9YrIUkw4ZFr7aUf1wVkswjFX8sGHFyKXtZ5hrLI
YwQIAJaYseiHhrDSEfSbja7w428aRaYuKFFhrsu2akWglg88pV4KJkld9OLE7wwi
ifzqymYE8hzE06HnmTcpej4kuxBNgcthrZlSSsOaMxsPK9fSliFzTOVEy9xNIT+L
orlK/ZDnoXWkJ8nCIWmXgmgbOAXt8lGxu5ROxESFNVwThUO5GXwoLQyDye0l11lj
Dt3gqKWBMO+Cro/Ez6Am1+yeUEoyHVTxjDKfGwFpqKA0r6qBjBO+HUJ2EB6l/hpc
ZorSredtZkWcTBQYU6eLqcjPNEIDBO7sE7iGL5DUw8V1rFFdCZLv8hKI6Fls8b2q
7KnMz+QstNql00TNLV6/liqwL4rBwU4DPzG+PxIQqf4QCACbrFk3ikMLI+X2Qd/T
SqSh6mEDpngx8ZG1CyPtD181d0lRwQPqtstnOfv32ytUjUqblHx7qmoxtmlbpmQj
enU+qFKP/SWfgXSGh7TQQm6EpWbrQfuBwbaB4fMYVZ26gk+3lsCWtMR18YI/orH+
llkA1bjF8N5+kKnIBcb6IK6u3udaQwEWOVAfhbdcRzU5xdxcxY7IUacRK9YV3YII
HBx3zZ/AgePngHEb4dm4oTuzy/DA3dMaNXHDSfrCA9xuAo/dXWelvIruk+CG01I0
fxyqex33lZ6qaS8/Cd/TU3jvpnnBn9iHbLY4Aa/909ag4ekVldMpzMUUwfSm6A1Q
pOtRB/9Tu+uiYKYfjvRqTk9bEjGYgYhoF/BcUI5FFYm7g7ldH+KHTaONH3us6Wj
YqlHSaVPFAWxwBVlaKTIwLgicwggHiuQdXFv/8oJBhIEPXT3/M3s0NfEqxcXOfhJ
CcxlwF0fcp182cGYWN8fRThJrL+6JKvep90AiRYEstRU/a0yfVCeqJlIXqxzgEtR
OPt+odWloFBEvYoWckxzBwa1CnBA/8TPxsZYcgOH7t9vOHl4X7d/tPKrrDEpZtyX
fYuwW4/WtNQucGBDsn6LL/3f0MsiYH487MwMp5MMGxluwQdjRqhKlG2C0lCGytBe
p3XgZLpS4HTYcgqcBuzBLOpnCUuP0sVkAdbyz5waT31OhnaqFoyNC8Zw7e9NVFJh
QStHp//stmUq35bE2GBf27lyGbezRSTC9YHYDOvNoOpBxbfc4seMBB8DuudYVwif
hqLO5DI/gDUr52rnzVNH9dGtvkVvFl+IYXNyKudmXoN21xS7BOcc9NB25Gw26x7h
6anz7Zrtsh/KvA5IVfmRPEQJQBjvsvi6iDht6i8bh0BJfAp0ov/Mksnjo029nAhD
Omh9irRFHLQrOWr1jj6+HovSQ7iummsfDC9byUqmKyEh6kLOZUfJK15EkJI3Z7rc
NAhpe0l2JqhspgZv4PCrWIHlHfHLU+G1U+Hg2Ewtz+G5HKmP0ucyQ0hgxy5DsaJl+

b0D7h00pFEDC8YykhT0RztxcKRBht64i4uVnNZodwk0qz4+96qo+keDugoNLysl
/P4HJisRhCmnsIOfwfy2pJXd9NcirxrR7+llDTQ0UrZqgkpNqxm5frMmslFtxmBq
LyRDtDSnKvLg4VxuOT5Q77cd4l3Re4qOh9YDtw+0+b/Bpg1B4CaE0kAR8Mgo2+Oq
7tbfz+7pUKyv8kc5/g5V0jjv1Gp6EyX6ocY6giYdWlmfz2PTpJDd24khd7DGruVg
+Z/a8XQmLhfLxwmC8FN4b67nbD9vGwNI0vQNbkl2hraD4tZaH7FUpT3WCy3qSwwP
SrC1+nElbRUIrFMor7AH9+gt0+/Fxa9OTaf1Zt0TLAsaP3Ze+c2OL+v3UJXksMm/
1YbrfZlsbJTaEWgr2ZAIHBUIE8J1H+zwT6nE+JNpn7lMi8pVcVlgjHMk8NZ/n/O/
EP9LesZeUY3T0dt6JD+ef3sDUADXIUFFLf2ruZ37A/BtZ8EJ9TMSUNz36woVnl0N
d8/57RqVRhooWOSFGBhlJcsF8HV1KJiwCcSFTTh21L3wd9FPel3wkZFCoQmJprSto
PbeqiBUmHqPeS3AvzQZMttUXSboBW9k5we2Gg6BtixPu1LbXgHZu/2GbGmLYG77Z
zni7kqDBx9866p+DGt0tHc0Jsl9746l5pGd/X79iRDoz/cpsltrUwdgQERicgDVC
UDhhHaHD8k12f7t08w3mWd4/vVDnz/SSB0MUD7l+HaXeuvJKswC4J1ip4FK5tmQJ
LmarV0W6FhbmdVQzTDCdDPaGb6E2oPnAVd6nasGdFXXwL2STbsRNTmVA09Wqi9ou
lZloeQGBbzhsFay+Vc+7XCxMmDm7lkt5WbZsYg9/x55/Vtkl5vRHPndTYvl+4N1e
OVyp88wmTzOjVXRHPxqsiksRQcYhEAPwD+knkkKumPNV0aXgWCxVCNHdk+G8d/Oj
6QVSe/ghbync1lG5JoJA2l67VfHG7h7UNZqu+bQJnJZlUhl4bFQecwbBgOREUYZ
svx0M4Q7py/ZCoyuF4u/Mm72dKpLOZ2c0CuDrjpboKHBO4NNMblQTILNeU8E0VhF
xBApQyrYtjsY0LIP+C6ZzF+MHtlS2C2wuWZlN60rvQGqVZlCvA/fgFKte9aFl1zY
zjCnlkgFAwKJfQlsXlPhoy0PqkEnyvk3NhiZtwZY8Wvy+nKm0glSD7fO71gdsL/q
UzcYr5EzUwr8hcPHvF8iyzHklpnt/E61s+DKdiVtfX9B7MZmT4C4yutWkrpy7kjM
EGPDqSOX3N2vX+qocSg7Fo69SGPRdsqrHROTINEBermzY+Od5Jdv5suUd6J4yen6
iEPcoAlCdvjdjWj9LmOCyE0wHbk1CzLM4S7fHc/LAwp4sp5SxZ3aXjjaTnk20ufG
9/MSzmSEOb7a5pQUnaircPPZiNOVP/pWQpKpnLY4eb8t0K1nDWLF5XgLWmrWD7lw
FFM73R0xD3P+kbhn6TTzBs1/vr8shXjL1zp9Gnbz/Tviw7LzWj4fhBKg4Z46BSZX
EB7wzc9lFhVHQDZDcJ//Cvqp1oTy+4QwgDvLbaXtNDdix71dws11fKRG8CIR5iNZ
X9ltMmrEupnk8qeX9J/nzv1f223k3tlisH3UVy1y1FL0Mld13xt/zNMiphK6OUuC
GEmMQlDonjVe4/L5ncUdmXfTNZcHzrs1/CuAGiddBwzmWHT9wTGHmrWKKs7s3qpG
NlgcU6LlhQVkkIC1
=2r7D
-----END PGP MESSAGE-----

Breault, Stephen

From:	[redacted]	s.16(2)(c)
Sent:	Tuesday, November 15, 2011 10:09 PM	
To:	[redacted]	
Cc:		s.19(1)
Subject:	RE:AC-2971 potential security issue in osCommerce	s.20(1)(c)

Bonjour, Good day,

Have you had a chance to look into this potential issue ? Here are some additional details:

Modules potentially affected:

[redacted]

Code:

[redacted]

Other similar modules:

[redacted]

Breault, Stephen

From: [REDACTED]
Sent: Thursday, November 17, 2011 10:31 AM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: FW: [security] AC-2971 Potential Security Issue affecting Ubercart for Drupal

This came into the [REDACTED] inbox for you.

s.16(2)(c)

Filing under AC-2971

s.19(1)

s.20(1)(c)

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca

"Patience isn't a skill — it's a decision"

-----Original Message-----

From: [REDACTED]
Sent: November 16, 2011 8:05 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: [security] AC-2971 Potential Security Issue affecting [REDACTED]

On Tue, Nov 15, 2011 at 9:33 PM, [REDACTED] wrote:

> Hi Matt, my turn to apologize for the slow turn around on your request.

>

> Yes, it is a [REDACTED] and it

> could be related to some of the subtitles of packaging x509 properly

> and maintaining associated certificate stores. However, this is

Breault, Stephen

From: [REDACTED]
Sent: Wednesday, November 16, 2011 8:05 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: [security] AC-2971 Potential Security Issue [REDACTED]

On Tue, Nov 15, 2011 at 9:33 PM, [REDACTED] wrote:

> [REDACTED] my turn to apologize for the slow turn around on your request.

>

> Yes, it is a [REDACTED] and it

s.16(2)(c)

> could be related to some of the subtitles of packaging x509 properly

s.19(1)

> and maintaining associated certificate stores. However, this is

s.20(1)(c)

> potentially problematic if not done. Other packages have acknowledged

> this issue and issued a fix.

>

> I am not aware of wrapping code which may supersede the PHP cURL SSL

> verification process in the current code, but you are far more

> knowledgeable of your package-suite than us.

>

> Have you been able to confirm the issue in current version ?

>

> Luc Beaudoin, P.Eng, MSc, MBA

> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

> Cyber Incident Response Centre | Centre canadien de réponse aux

> incidents cybernétiques Public Safety Canada | Sécurité publique

> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur

> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government

> of Canada | Gouvernement du Canada

>

>

> From [REDACTED]

> Sent: November 4, 2011 1:59 AM

> To [REDACTED]

> Subject: [REDACTED]

s.16(2)(c)

s.19(1)

s.20(1)(c)

>
> Luc-
> Sorry for the delay.
> I have not gotten a change to take a look at it further in depth, but
> the issue makes sense and might extend [REDACTED]
> [REDACTED] is
> this the way the code is written in the gateway's example code? (I'll
> be checking into it further, but thought that off hand you probably
> know better than I
> do)
> Thanks
[REDACTED]
>
>
> On Wed, Nov 2, 2011 at 1:40 PM [REDACTED] wrote:
>>
> [REDACTED] I am following up on the information sent to you last week. Did
>> you get the chance to review/confirm the potential security issue
>> associated with current modules reported ?
>>
>> Luc
>>
>> Luc Beaudoin, P.Eng, MSc, MBA
>> Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>> Cyber Incident Response Centre | Centre canadien de réponse aux
>> incidents cybernétiques Public Safety Canada | Sécurité publique
>> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur
>> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
>> Government of Canada | Gouvernement du Canada
>>
>>
>>
>> _____
>> From: Beaudoin, Luc S
>> Sent: October 28, 2011 12:44 PM
>> To: [REDACTED]
>> Subject: RE: [REDACTED]
[REDACTED]
>> Importance: High
>>
>> Matt,
>>
>> We were informed by a researcher that the [REDACTED]
>> to verify SSL certificate in various modules may be unsecured due to
>> the VERIFYPEER option being set to False by default.
>>
>> Specifically, modules such as:
>>
[REDACTED]

>>

>> seem to use the following code: curl_setopt(\$ch,
>> CURLOPT_SSL_VERIFYPEER, 0);

s.16(2)(c)

>>

>> This line may prevent SSL certificate validation between the
>> merchant's server and the transaction processor.

s.19(1)

s.20(1)(c)

>>

>> We would like to raise awareness of this coding practice amongst key
>> ecommerce package development community to avoid server-to-server
>> communications being potentially vulnerable to m-i-m attacks.

>>

>> I would like to know what your thoughts are on this and if your
>> community would consider changing these settings with a default
>> setting which would ensure SSL certificates are validated.

>>

>> thanks

>>

>> Luc

>>

>> Luc Beaudoin, P.Eng, MSc, MBA

>> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>> Cyber Incident Response Centre | Centre canadien de réponse aux

>> incidents cybernétiques Public Safety Canada | Sécurité publique

>> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur

>> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca

>> Government of Canada | Gouvernement du Canada

>>

>>

>>

>>

>> From: [REDACTED]

>> Sent: October 28, 2011 12:26 PM

>> To: [REDACTED] Beaudoin, Luc S

>> Subject: Re: [REDACTED]

>>

>>

>> Luc-

>>

>> The [REDACTED] will deal with security issues and work out

>> a fix in private, you've reached the [REDACTED]

>> This is the proper venue for reporting such an issue.

>>

>> Please provide details of the issue.

>>

>> Thanks

>>

s.16(2)(c)

>>

>>

s.20(1)(c)

>> On Wed, Oct 26, 2011 at 12:59 PM, Beaudoin, Luc S

>> <Luc.Beaudoin@ps-sp.gc.ca> wrote:

>>>

>>> Good day,

>>>

>>> Could you assist us with identifying the best mechanism/contact to

>>> bring forward a potential security issue

>>>

>>> Thank you

>>>

>>>

>>> Luc Beaudoin, P.Eng, MSc, MBA

>>> Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>>> Cyber Incident Response Centre | Centre canadien de réponse aux

>>> incidents cybernétiques Public Safety Canada | Sécurité publique

>>> Canada Telephone | Téléphone +1 613-991-9949 Facsimile |

>>> Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca

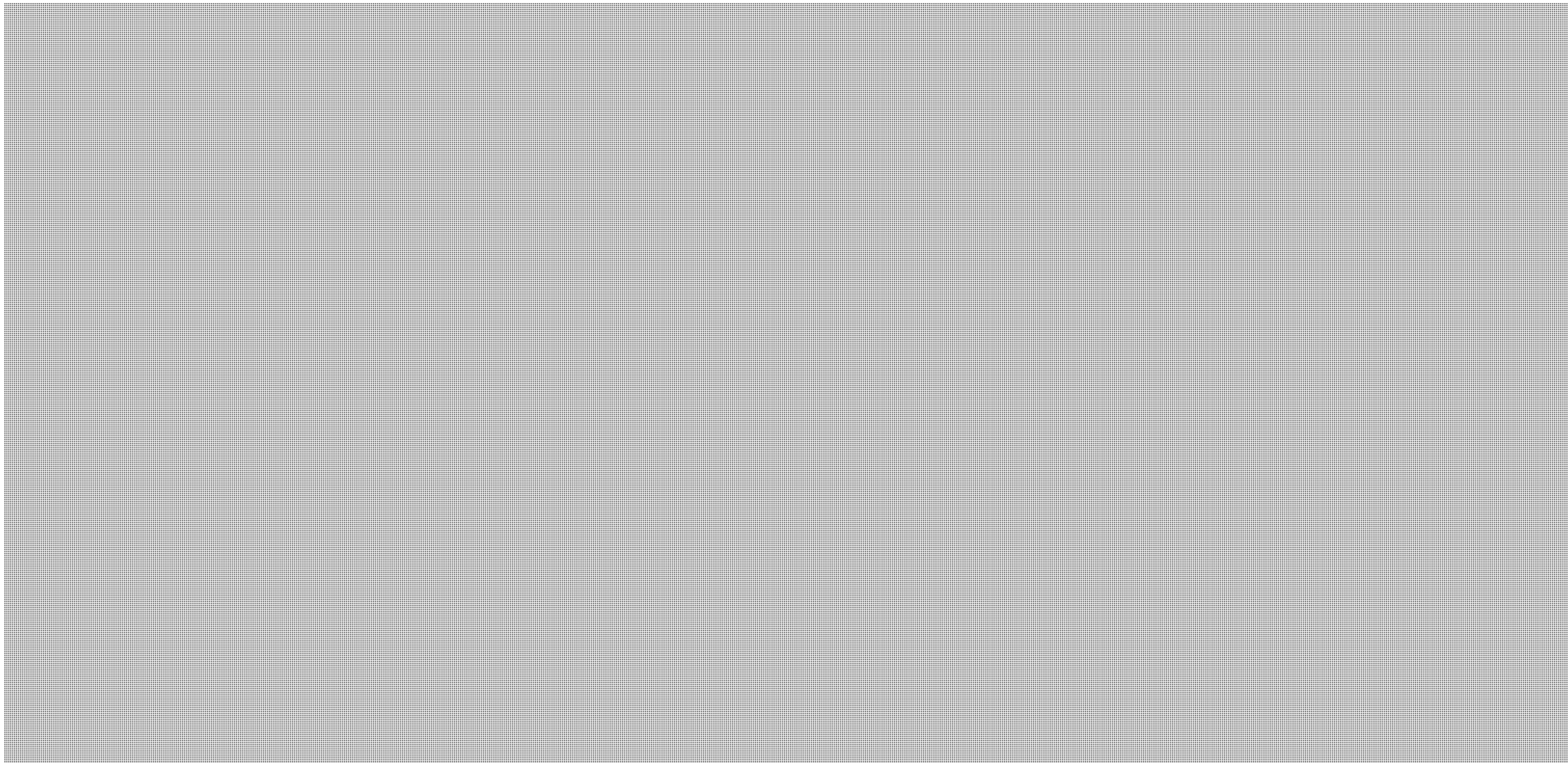
>>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

>>>

>>>

>>>

>>> --



Breault, Stephen

From: [REDACTED]
Sent: Thursday, November 17, 2011 11:29 AM
To: [REDACTED]
Subject: Re: 2971: Notification [REDACTED] potential security issue, update

s.16(2)(c)

On 11/15/11 8:32 PM, "CYBERDO" <CyberDO@ps-sp.gc.ca> wrote:

s.19(1)

>I [REDACTED] it seems there may still be an issue with the [REDACTED]

s.20(1)(c)

>the VERIFYPEER setting to False.

>

>Would you be able to confirm, or indicate otherwise ?

>

>Thanks !

>

>

>Luc Beaudoin, P.Eng, MSc, MBA

>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>Cyber Incident Response Centre | Centre canadien de réponse aux

>incidents cybernétiques Public Safety Canada | Sécurité publique Canada

>Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1

>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of

>Canada | Gouvernement du Canada

>

>-----Original Message-----

>From [REDACTED]

>Sent: November 3, 2011 12:39 PM

>To [REDACTED]

>Subject: Re: 2971: Notification [REDACTED] potential security issue,

>update

>

[REDACTED]

>

[REDACTED]

>

>On 10/26/11 12:11 PM, [REDACTED] wrote:

>

>>Thanks [REDACTED]

>>

>>Could you send us the link for the update if/when available ?

>>

>>Luc Beaudoin, P.Eng, MSc, MBA

>>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>>Cyber Incident Response Centre | Centre canadien de réponse aux
>>incidents cybernétiques Public Safety Canada | Sécurité publique
>>Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur
>>+1
>>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of
>>Canada | Gouvernement du Canada

s.16(2)(c)

>>

>>

s.19(1)

>>

s.20(1)(c)

>>-----Original Message-----

>>From: S [REDACTED]

>>Sent: October 26, 2011 1:44 PM

>>To [REDACTED]

>>Subject: Re: 2971: Notification [REDACTED] security issue,

>>update

>>Importance: High

>>

>>The necessary option has been changed in the package. It should be

>>uploaded soon if it has not been already.

>>

>>

>>On 10/26/11 9:30 AM, [REDACTED] wrote:

>>

>>>Good day [REDACTED]

>>>

>>>I was wondering if you had an update on the info we passed to you at

>>>the beginning of the month. I am attaching an advisory which we

>>>intend on posting to our website next week. I would appreciate any

>>>comments, advice or recommendations your organisation may have with

>>>regard to this advisory.

>>>

>>>The site link where this advisory would be posted is:

>>><http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>

>>>

>>>Note that the researcher who brought this issue to our attention

>>>intends on posting it in various technical communities to raise

>>>awareness.

>>>

>>>Please advise.

>>>

>>>Luc

>>>

>>>Luc Beaudoin, P.Eng, MSc, MBA

>>>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>>>Cyber Incident Response Centre | Centre canadien de réponse aux

>>>incidents cybernétiques Public Safety Canada | Sécurité publique

>>>Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur

>>>+1

>>>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government

>>>of Canada | Gouvernement du Canada

>>>

>>>

s.16(2)(c)

Breault, Stephen

From: Scouten, Julia
Sent: Monday, November 21, 2011 8:09 AM
To: Beaudoin, Luc S
Cc: [REDACTED]
Subject: RE: Activyt 3271: for translation

Good Morning Luc,

I sent this document , with Rhonda's edits, for translation on Friday. Haven't heard anything back yet, so I emailed them again.

Will let you know,

Julia Scouten CISSP GCIA GCIH GSEC
Incident Handler
Canadian Cyber Incident Response Centre (CCIRC) Public Safety Canada Julia.Scouten@ps-sp.gc.ca
613-991-7070

From: Beaudoin, Luc S
Sent: Sunday, November 20, 2011 11:10 PM
To: [REDACTED]
Cc: Scouten, Julia
Subject: Activyt 3271: for translation

<< File: IN11-XXX_EN cURL_VERIFYPEER.txt >>

I reviewed and integrated Rhonda's comments. Send to translation. NO DISTRIBUTION YET.

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Breault, Stephen

From: [REDACTED]
Sent: Monday, November 21, 2011 12:06 PM
To: Beaudoin, Luc S
Cc: [REDACTED] Scouten, Julia
Subject: FW: (for review) CCIRC COMBINED Language INFORMATION NOTE IN11-XXX
Translation Request
Attachments: IN11-XXX_PHPcURL_VERIFYPEERv2.txt; 2011-11-21 8278956_FR_2011_11_18_IN11
_XXX_PHPcURL_VERIFYPEERv2.txt

Your last email said "NO DISTRIBUTION YET"

Please advise when & who for Dist. thanks!

Sandra Williston, GCIH
Incident Handler
Canadian Cyber Incident Response Centre
Public Safety Canada
Tel: (613)991-7039 Fax: (613)991-3574
www.PublicSafety.gc.ca <<http://www.publicsafety.gc.ca/>>

"Patience isn't a skill — it's a decision"

From: [REDACTED]
Sent: November 21, 2011 11:12 AM
To: [REDACTED]
Subject: (for review) CCIRC COMBINED Language INFORMATION NOTE IN11-XXX Translation Request

Attached French translation.

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

From: [REDACTED]
Sent: November 18, 2011 12:07 PM
To: [REDACTED]

Cc: [REDACTED]

Subject: CCIRC COMBINED Language INFORMATION NOTE IN11-XXX Translation Request

Attachment: IN11-XXX_PHPcURL_VERIFYPEERv2.txt

GOC,

****NOTE:** A combined language version of this product will be sent once the translation has been received and reviewed.**

The following steps are requested for this CCIRC product:

1. Please send the attached English version, minus the Note to Readers, for translation. After hours translation is NOT required.
2. Once returned, the GOC will forward the translated version of the product back to the [REDACTED] for review and additional instructions. Please ensure the subject line of the email for the [REDACTED] contains the additive "For your Review".
3. Distribution instructions will be provided after the [REDACTED] completes their review.

Thank you,

CyberDO

**Pages 227 to / à 228
are withheld pursuant to section
sont retenues en vertu de l'article**

21(1)(a)

**of the Access to Information
de la Loi sur l'accès à l'information**

Pages 229 to / à 230
are withheld pursuant to sections
sont retenues en vertu des articles
16(1)(b), 16(2)(c), 20(1)(c), 21(1)(a)
of the Access to Information
de la Loi sur l'accès à l'information

2011-11-21 8278956_FR_2011_11_18_IN11_XXX_PHPcURL_VERIFYPEERV2

SÉCURITÉ PUBLIQUE CANADA
CENTRE CANADIEN DE RÉPONSE AUX INCIDENTS CYBERNÉTIQUES

NOTE D'INFORMATION

Numéro : IN11-XXX
Date :

Mise en œuvre de l'option Verify Peer de la bibliothèque PHP CURL dans les
applications qui requiert la vérification du certificat SSL

OBJET
=====

Le présent avis vise à attirer l'attention sur une mise en œuvre courante, mais non
sécurisée de l'option CURL PHP utilisée pour vérifier des certificats SSL.

ÉVALUATION
=====

Le langage PHP (préprocesseur hypertexte) est un langage de script côté-serveur
adaptable. Il permet au développeur de générer des pages HTML de manière dynamique.
Le langage PHP implante plusieurs bibliothèques de codes standards, notamment CURL
(Client URL Request Library ou libcurl). Cette dernière comprend un ensemble de
fonctions pour établir des connexions avec différents protocoles, dont HTTPS. Elle
est également responsable de la mise en place de caractéristiques de sécurité, comme
la validation des certificats SSL au moment d'établir des connexions HTTPS. Elle est
couramment utilisée par les développeurs d'applications web (p. ex., les
applications de commerce électronique) pour établir une connexion sécurisée entre
des systèmes hébergés sur différents segments du réseau, notamment la connexion à un
service tiers de traitement des cartes de paiement.

Dans la bibliothèque, la fonction curl_setopt permet de régler plusieurs options
d'exécution, comme la configuration de la vérification des certificats SSL selon les
autorités de certification (AC) pertinentes. L'option CURLOPT_SSL_VERIFYPEER
détermine si la bibliothèque va tenter de valider l'approbation des certificats SSL
au moment de l'établissement de connexions sécurisées. Lorsque la bibliothèque CURL
essaie de vérifier le certificat d'un serveur à distance auprès des AC approuvées
conformément à l'option de configuration CURLOPT_CAINFO ou CURLOPT_CAPATH. L'option
CURLOPT_SSL_VERIFYPEER est activée par défaut et, sur certaines plateformes, une
liste des AC est prédéfinie. Or, ce cadre de validation est souvent désactivé par le
développeur qui règle le paramètre de l'option CURLOPT_SSL_VERIFYPEER à « 0 » ou «
Faux ». Si la vérification par les pairs est désactivée, les certificats SSL ne sont
pas vérifiés pour approbation par la bibliothèque CURL. La non-validation des
certificats SSL par l'application ouvre la porte à différents scénarios d'attaque de
l'intercepteur (man-in-the-middle attack), ce qui peut mener à l'interception et à
la modification des données en transit.

Les fonctions CURL sont fréquemment utilisées dans le cadre de communications
serveur à serveur et, par conséquent, l'opérateur d'application (p. ex., un marchand
qui exploite un commerce électronique) peut ignorer que ses applications font
peut-être des transactions sur des canaux de communications non sécurisés.

2011-11-21 8278956_FR_2011_11_18_IN11_XXX_PHPCURL_VERIFYPEERV2

Les progiciels
étant habituellement fournis en code source, le développeur et l'opérateur du site
doivent s'assurer que les fonctionnalités de sécurité sont activées conformément à
la sensibilité et aux attentes en matière de protection des données transmises.

MESURES RECOMMANDÉES

=====

Le CCRIC recommande aux opérateurs d'applications web qui mettent en œuvre les
connexions TLS/SSL au moyen de la bibliothèque PHP CURL de vérifier que la valeur
booléenne de l'option CURLOPT_SSL_VERIFYPEER soit réglée à Vrai ou à la valeur
correspondant au nombre entier 1 et de régler les paramètres de manière à ce que
l'échec d'obtention d'une vérification réussie entraîne une erreur d'échec de
connexion plutôt que l'établissement d'une connexion non approuvée et non sécurisée.
Il suffit de faire une recherche dans le répertoire de codes sources des
applications (voir les exemples d'entrées ci-dessous) pour obtenir des indications
sur les paramètres utilisés dans la mise en œuvre CURL :

Exemples :

```
curl_setopt($connection, CURLOPT_SSL_VERIFYPEER, 0,1,True or False);
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca-bundle.crt");
curl_setopt($connection, CURLOPT_CAINFO, "path:/ca.pem");
curl_setopt($connection, CURLOPT_CAPATH, "path:/");
```

Le CCRIC recommande que les organismes qui traitent des transactions examinent leurs
API en langage PHP distribuées et qu'ils s'assurent que les API font respecter la
mise en œuvre adéquate de la vérification des certificats par les marchands et les
partenaires affiliés.

Dans la mesure du possible, les développeurs de NIP d'applications sécurisés doivent
certifier la validation selon le certificat d'AC qui sera utilisé. Cela peut être
accompli en utilisant l'option CURLOPT_CAINFO et en distribuant le certificat public
associé de l'AC et le code de programme dans le même progiciel. Veuillez consulter
les documents de références ci-dessous pour obtenir des renseignements détaillés sur
la mise en œuvre.

Le CCRIC recommande que les opérateurs d'applications web vérifient régulièrement la
disponibilité des mises à jour et des correctifs des progiciels et qu'ils les
mettent à l'essai et les déploient adéquatement en temps opportun.

SOURCES

=====

Le CCRIC désire remercier Kevin McArthur de StormTide Digital Studios Inc. et Tamir
Israel de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC)
pour leurs recherches et leur contribution à ce produit.

Références :

=====

```
http://curl.haxx.se/
http://curl.haxx.se/docs/sslcerts.html
http://curl.haxx.se/docs/caextract.html
http://php.net/manual/en/function.curl-setopt.php
http://www.openssl.org/docs/apps/x509.html
http://www.openssl.org/docs/ssl/SSL_CTX_load_verify_locations.html
```

Pages 233 to / à 234
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c), 21(1)(a), 21(1)(b), 23

of the Access to Information
de la Loi sur l'accès à l'information

Breault, Stephen

From: Beaudoin, Luc S
Sent: Thursday, November 24, 2011 2:57 PM
To: [REDACTED]
Subject: Re: curl

Ack

Luc Beaudoin

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----

From: S [REDACTED]
Sent: Thursday, November 24, 2011 02:56 PM
To: Beaudoin, Luc S
Subject: RE: curl

Thanks and here is my PGP key.

Cheers,

-----Original Message-----

From: Beaudoin, Luc S [<mailto:LucS.Beaudoin@ps-sp.gc.ca>]
Sent: 2011, November, 24 12:07 PM
To: [REDACTED]
Subject: curl

Thanks for your reply and yes, please do along with the N1 accordingly.

I don t have your PGP...

Luc

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----

From: [REDACTED]

Sent: November 24, 2011 11:59 AM

To: Beaudoin, Luc S

Subject: CURL

s.19(1)

s.20(1)(c)

* PGP Decrypted Message

Hi Luc,

[REDACTED]

Cheers,

[REDACTED]

[REDACTED]

Breault, Stephen

From: Beaudoin, Luc S
Sent: Friday, November 25, 2011 2:24 PM
To: Scouten, Julia
Subject: RE: Update on Products in the Queue

for the APT one, we need to transpose it into our txt product format, bilingual. Could you do it please ? We ll release next week.

L

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: Scouten, Julia
Sent: November 25, 2011 10:32 AM
To: Beaudoin, Luc S
Subject: Update on Products in the Queue

Hi Luc,

Here is a summary of our products that still needs to be closed off.

TR11-002 – Mitigation Guidelines for Advanced Persistent Threats

s.20(1)(c)

- English and French version saved in portal under TR11-002
- Not distributed, but sent to [REDACTED] and Stephane at TBS

IN11-003 - Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification

- English and French version saved in portal under IN11-003 (wasn't sure if it should be 500 series or not)

- Not distributed.

CF11-xxxx - Summary of Recent Spear Phishing Campaigns and potential APT indicators

- No translation.
- Still in draft stage. Latest update is your draft.
- Saved in portal.

DDoS Mitigation Paper

- Saved under Technical Reports, but it says it's an Information Report. Need to clarify.
- No translation.
- No distribution.

I have also attached all copies just in case they get "lost" somewhere.

Julia Scouten CISSP GCIA GCIH GSEC

Incident Handler

Canadian Cyber Incident Response Centre (CCIRC)

Public Safety Canada

Julia.Scouten@ps-sp.gc.ca <<mailto:Julia.Scouten@ps-sp.gc.ca>>

613-991-7070

Breault, Stephen

From: Beaudoin, Luc S
Sent: Friday, December 02, 2011 7:16 AM
To: Covo, Pierre
Subject: cURL write up

Did you get the chance to send something to my exec ? (Robert Dick and Windy Anderson)

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Pages 240 to / à 242
are withheld pursuant to sections
sont retenues en vertu des articles

16(2)(c), 20(1)(c), 21(1)(a), 23

of the Access to Information
de la Loi sur l'accès à l'information

s.19(1)

Breault, Stephen

From: Beaudoin, Luc S
Sent: Friday, December 16, 2011 6:00 PM
To: [REDACTED]
Subject: Re: Any progress?

Yes of course. [REDACTED].although I appreciate t [REDACTED] wished we
[REDACTED]

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [REDACTED]
Sent: Friday, December 16, 2011 04:33 PM
To: Beaudoin, Luc S
Subject: RE: Any progress?

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca]
Sent: December 16, 2011 4:10 PM
To: [REDACTED]
Subject: RE: Any progress?

s.19(1)

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: December-15-11 5:55 PM
To: Beaudoin, Luc S
Subject: RE: Any progress?

[REDACTED]

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca] <mailto:%5bmailto:LucS.Beaudoin@ps-sp.gc.ca%5d>
Sent: December 15, 2011 5:53 PM
To: [REDACTED]
Subject: Re: Any progress?

Agreed. I can emphasize this. I ll resend tomorrow.

Luc Beaudoin

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: [REDACTED]
Sent: Thursday, December 15, 2011 03:57 PM
To: Beaudoin, Luc S
Subject: RE: Any progress?

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca] <mailto:%5bmailto:LucS.Beaudoin@ps-sp.gc.ca%5d>
Sent: December 15, 2011 3:52 PM
To: [REDACTED]
Subject: RE: Any progress?

No need to apologies. I very much respect your dedication and involvement in this file. I am sorry for the delays. I got my final marching orders this morning. This is the final draft which I am authorized to post now.

Question: are you guys still OK with the credit ?

DRAFT (for your information only until officially posted):

La version française suit

PUBLIC SAFETY CANADA

CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

s.16(2)(c)

s.19(1)

Government Operations Centre/

Centre des opérations du gouvernement

Email/courriel [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

From: [REDACTED]

Sent: December-15-11 3:04 PM

To: Beaudoin, Luc S

Subject: RE: Any progress?

From: Beaudoin, Luc S [mailto:LucS.Beaudoin@ps-sp.gc.ca] <mailto:%5bmailto:LucS.Beaudoin@ps-sp.gc.ca%5d>

Sent: December 15, 2011 10:31 AM

To: [REDACTED]

Subject: RE: Any progress?

I am meeting my exec today on this topic following reception of legal staff recommendations. Will have more info this PM.

s.19(1)

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques
Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone +1 613-991-9949
Facsimile | Télécopieur +1 613-991-3574
luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>
PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: December-14-11 9:01 PM
To: Beaudoin, Luc S
Subject: Any progress?

P Do you really need to print this email? / Est-ce nécessaire d'imprimer ce courriel?

Breault, Stephen

From: Beaudoin, Luc S
Sent: Wednesday, December 21, 2011 3:33 PM
To: Cameron, Bud
Subject: Re: CCIRC IN11-003 Implementing PHP cURL Verifypeer Option in Applications
Requiring SSL Certificate Verification / Mise en œuvre de l'option Verify Peer de la
bibliothèque PHP cURL dans les applications qui requiert la vérification du certificat SSL

No. These are open source projects provided in source code which is literally cut and pasted into server platform code before compiling it.

Luc Beaudoin

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

----- Original Message -----

From: Cameron, Bud
Sent: Wednesday, December 21, 2011 11:58 AM
To: Beaudoin, Luc S
Subject: FW: CCIRC IN11-003 Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate
Verification / Mise en œuvre de l'option Verify Peer de la bibliothèque PHP cURL dans les applications qui requiert la
vérification du certificat SSL

Just for my own edification, isn't "source code" the high level programming language text? Didn't you mean to say that
software programs are delivered in compiled form (binary, executable) so you can't easily check if the security function
is disabled? If so, not worth a correction, the overall meaning is clear.

s.16(2)(c)

-----Original Message-----

From: [REDACTED]
Sent: December-20-11 1:52 PM
To: [REDACTED]
Subject: CCIRC IN11-003 Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification
/ Mise en œuvre de l'option Verify Peer de la bibliothèque PHP cURL dans les applications qui requiert la vérification du
certificat SSL

(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

UNCLASSIFIED
FOUO

CCIRC Daily Situation Report

Date: 21 Dec 11

CYBERDO: Vireak

[FOUO] EVENTS:

1. Title: CE11-2542 [XSSED Notification]

Action/Decision: CCIRC observed that a webpage allocated to a Canadian union was listed on XSSED.com as containing cross site scripting vulnerability.

A. Item: A notification was sent to the technical contact recommending that all web pages using external data such as web forms, parameters or cookies should be audited for cross site scripting and SQL injection vulnerabilities.

- Owner: Bruce
- Status: Closed

2. Title: CE11-2543 [XSSED Notification]

Action/Decision: Report received from XSSed.com that a webpage allocated a Federal department was listed on XSSED.com as containing cross site scripting vulnerability.

A. Item: Notification sent to CTEC recommending that all web pages using external data such as web forms, parameters or cookies should be audited for cross site scripting and SQL injection vulnerabilities.

- Owner: Bruce
- Status: Closed

[FOUO] ACTIVITIES:

[FOUO] INTERNATIONAL PARTNERS:

1. Item Description: ICSA-11-332-01 - Invensys Wonderware InBatch ActiveX Vulnerabilities

CYBER ENVIRONMENT SCANNING:

Websites

Malicious Activities and Incident Reports :

Atlas Canada Report (<http://atlas.arbor.net/cc/CA>)

ShadowServer Reports – previous day activity

Zeus Tracker (<https://zeustracker.abuse.ch/index.php>)

SpyEye Tracker (<https://spyeyetracker.abuse.ch/monitor.php>)

XSSED (<http://xssed.com/archive/special=1>)

Zone-H - Special Defacements (www.zone-h.org/archive/special=1)

Vulnerabilities:

Secunia (<http://secunia.com/advisories/historic/>)

Checked
(Y/N)

N

N

Y

Y

Y

Y

Y

UNCLASSIFIED
FOUO

UNCLASSIFIED
FOUO

Vupen (http://www.vupen.com/english/security-advisories/)	Y
Security Tracker (http://securitytracker.com/archives/summary/9000.html)	Y
http://blogs.technet.com/b/msrc/	Y
http://web.nvd.nist.gov/view/vuln/search-advanced?cid=2	Y
News and Trends:	
http://threatpost.com/	N
http://blog.trendmicro.com/	N
SANS (http://isc.incidents.org/)	N
Sucuri Blog (http://blog.sucuri.net/)	N
F-Secure (http://www.f-secure.com/weblog/)	N
Topix News (http://www.topix.net/tech/computer-security)	N
News Now (http://www.newsnow.co.uk/h/Technology/Computer+Technology/Security)	N
The H Security (http://www.h-online.com/security/news/)	N
The Register (http://www.theregister.co.uk/)	
http://www.securityfocus.com/bid/	
	N
Sophos Blog (http://nakedsecurity.sophos.com/)	N
http://seclists.org/isn/	N

PUBLICATIONS: CCIRC IN11-003 Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification [released to all cyber clients and posted on public website]

VULNERABILITY WATCH:

1. Item Description: Microsoft Windows win32k.sys Memory Corruption Vulnerability – While using the Apple Safari browser, a user visiting a crafted page that includes an IFRAME containing a large height attribute, it can allow for remote code execution with kernel-mode privileges. It has been confirmed and the vulnerability exists on a fully patched WIN 7/64 OS. NO CVE. No patch available.
- Reference: <http://secunia.com/advisories/47237/>

THREAT WATCH: NIL

CYBER NEWS:

1. Canada Post is warning its customers that a circulating email that claims price discrepancies between corporate and private postal outlets is fake. The email, purportedly from a customer, claims Canadians can ship the exact same packages out of corporate outlets for less. This is the second time the email has surfaced in more than a year, said Canada Post spokeswoman Anick Losier. The same email made the rounds last December. The corporation is also not sure whether the email is spam and where it originates from.
http://www.infomedia.gc.ca/ps-sp/articles/unrestricted/2011/12/ps-2011123326927326_4.htm

UNCLASSIFIED
FOUO

UNCLASSIFIED
FOUO

2. Title: Exploit Kits Now Updated With New Wares Before Patches Are Ready
"The creators and maintainers of exploit kits often rely on public reports of new exploits and proof-of-concept exploit code in order to be able to add new exploits to their software. And in many cases, the exploits included in kits such as Black Hole and Eleonore and others will be for vulnerabilities that are older and have long since been patched. But, if recent events are any indication, that could be changing. In mid-October, details of a new Java vulnerability emerged in various places, and descriptions of the flaw showed it to be a serious one that could lead to remote code execution. The CVE-2011-3544 vulnerability, though serious, was just one of many that had been found in various Java components in recent months, and there already were plenty of others in the exploit kits that were being used in attacks."

Source: http://threatpost.com/en_us/blogs/exploit-kits-now-updated-new-wares-patches-are-ready-122011

[FOUO] GENERAL INFORMATION:

GovIRT today

- Only the Vulnerability Watch, Threat Watch and Cyber News sections are publicly releasable;
- This daily report was reviewed and approved by:

UNCLASSIFIED
FOUO

s.16(2)(c)

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Thursday, December 22, 2011 12:57 PM
To: [REDACTED]
Subject: 2971: Notification PayPal API potential security issue, update-2

Good day [REDACTED]

I would like to draw your attention to the following recent publication related to this issue. If you have any questions or comments, feel free to contact us.

Cheers

Luc

URL: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

Content:
(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-003
Date: 20 December 2011

Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification

PURPOSE
=====

The goal of this Information Note is to raise awareness of a common but potentially insecure implementation of the PHP cURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (cURL or libcurl). The cURL library provides a set of functions that allows establishing connections using various communication protocols including HTTPS. This library is also responsible for implementing security features such as the validation of SSL certificates when

Centre des opérations du gouvernement

Email/courriel: [REDACTED]

s.16(2)(c)

s.19(1)

s.20(1)(c)

Government Operations Centre/

Centre des opérations du gouvernement

Email/courriel: [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----

From: [REDACTED]

Sent: November-23-11 12:10 PM

To: [REDACTED]

Subject: Re: 2971: Notification [REDACTED] potential security issue, update

Luc,

I have confirmed the issue and have asked for it to be corrected. I will send you an email when it has been corrected.

On 11/15/11 8:32 PM, [REDACTED] wrote:

[REDACTED] it seems there may still be an issue with the [REDACTED]
[REDACTED] with

>the VERIFYPEER setting to False.

>

>Would you be able to confirm, or indicate otherwise ?

>

>Thanks !

>

>

>Luc Beaudoin, P.Eng, MSc, MBA

>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>Cyber Incident Response Centre | Centre canadien de réponse aux

>incidents cybernétiques Public Safety Canada | Sécurité publique Canada

>Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1

>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of

>Canada | Gouvernement du Canada

>

>-----Original Message-----

>From: [REDACTED]
>Sent: November 3, 2011 12:39 PM
>To: [REDACTED]
>Subject: Re: 2971: Notification [REDACTED] potential security issue,
>update
>
> [REDACTED] have been updated.
>
>

s.16(2)(c)

s.19(1)

s.20(1)(c)

>
>
>On 10/26/11 12:11 PM, [REDACTED]
>
>>Thanks [REDACTED]
>>
>>Could you send us the link for the update if/when available ?
>>
>>Luc Beaudoin, P.Eng, MSc, MBA
>>Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>>Cyber Incident Response Centre | Centre canadien de réponse aux
>>incidents cybernétiques Public Safety Canada | Sécurité publique
>>Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur
>>+1
>>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of
>>Canada | Gouvernement du Canada
>>
>>
>>

>>-----Original Message-----

>>From: [REDACTED]
>>Sent: October 26, 2011 1:44 PM
>>To: [REDACTED]
>>Subject: Re: 2971: Notification [REDACTED] security issue,
>>update
>>Importance: High
>>
>>The necessary option has been changed in the package. It should be
>>uploaded soon if it has not been already.
>>
>>

>>On 10/26/11 9:30 AM, [REDACTED] wrote:

>>>Good day [REDACTED]

>>>

>>>I was wondering if you had an update on the info we passed to you at
>>>the beginning of the month. I am attaching an advisory which we
>>>intend on posting to our website next week. I would appreciate any
>>>comments, advice or recommendations your organisation may have with
>>>regard to this advisory.

>>>

>>>The site link where this advisory would be posted is:

>>>http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx
>>>
>>>Note that the researcher who brought this issue to our attention
>>>intends on posting it in various technical communities to raise
>>>awareness.
>>>
>>>Please advise.
>>>
>>>Luc
>>>
>>>Luc Beaudoin, P.Eng, MSc, MBA
>>>Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>>>Cyber Incident Response Centre | Centre canadien de réponse aux
>>>incidents cybernétiques Public Safety Canada | Sécurité publique
>>>Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur
>>>+1
>>>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government
>>>of Canada | Gouvernement du Canada
>>>
>>>
>>>
>>>-----Original Message-----
>>>From: [REDACTED]
>>>Sent: October 4, 2011 4:49 PM
>>>To: [REDACTED]
>>>Subject: Re: 2971: Notification [REDACTED] security issue
>>>Importance: High
>>>
>>>Luc,
>>>
>>>
>>>I have the proper key and have decrypted the message. We are
>>>reviewing the issue now. Thank you for your submission.
>>>
>>>On 10/3/11 11:32 AM, "[REDACTED]" wrote:
>>>
>>>>Thanks for the quick reply. Find details attached [REDACTED]
[REDACTED] We would appreciate your thoughts on this.
>>>>
>>>>Cheers
>>>>
>>>>Luc Beaudoin, P.Eng, MSc, MBA
>>>>Chief Cyber Operations | Chef des opérations cybernétiques Canadian
>>>>Cyber Incident Response Centre | Centre canadien de réponse aux
>>>>incidents cybernétiques Public Safety Canada | Sécurité publique
>>>>Canada Telephone | Téléphone +1 613-991-9949 Facsimile |
>>>>Télécopieur
>>>>+1
>>>>613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government
>>>>of Canada | Gouvernement du Canada
>>>>
>>>>

s.16(2)(c)

s.19(1)

s.20(1)(c)

>>>>Need to report an incident? Find the Incident Report Form here:

>>>>

>>>>

>>>><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti>

>>>>/

>>>>i

>>>>t

>>>>imp

>>>>-pgimti-app-ann-D-eng.rtf

>>>>

>>>>Vous voulez rapporter un incident ? Utilisez le formulaire de

>>>>déclaration

>>>>suivant:

>>>>

>>>><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti>

>>>>/

>>>>i

>>>>t

>>>>imp

>>>>-pgimti-app-ann-D-fra.rtf

>>>>

>>>>

>>>>

>>>>

>>>>-----Original Message-----

>>>>From: [REDACTED]

>>>>Sent: October 3, 2011 12:22 PM

>>>>To [REDACTED]

>>>>Subject: Re: 2971: Notification [REDACTED] potential security issue

>>>>Importance: High

>>>>

>>>>Luc,

>>>>

>>>>I am a member of the [REDACTED] Please

>>>>provide more information in regards to your discovery. Thanks.

>>>>

>>>>



s.16(2)(c)

s.19(1)

s.20(1)(c)

s.16(2)(c)

s.20(1)(c)

>>>>Date: Mon, 3 Oct 2011 09:52:37 -0600

>>>>To: [REDACTED]

>>>>Cc: [REDACTED]

>>>>Subject: 2971: Notification [REDACTED] security issue

>>>>

>>>>The Canadian Cyber Incident Response Centre (CCIRC) was recently
>>>>informed of potentially insecure implementations of APIs which are
>>>>used to access your services. CCIRC would like to raise your
>>>>awareness of this potential issue and seek your support in
>>>>mitigating any associated risks.

>>>>

>>>>Could you confirm who might be the most appropriate contact [REDACTED]

>>> [REDACTED] the technical details surrounding this issue to

>>>>(API applications development team maybe ?) and the associated PGP

>>>>key [REDACTED]

>>>>

>>>>thank you

>>>>

>>>>Luc Beaudoin, P.Eng, MSc, MBA

>>>>Chief Cyber Operations | Chef des opérations cybernétiques Canadian

>>>>Cyber Incident Response Centre | Centre canadien de réponse aux

>>>>incidents cybernétiques Public Safety Canada | Sécurité publique

>>>>Canada Telephone | Téléphone +1 613-991-9949 Facsimile |

>>>>Télécopieur

>>>>+1

>>>>613-991-3574

>>>>luc.beaudoin@ps-sp.gc.ca<mailto:luc.beaudoin@ps-sp.gc.ca>

>>>>PublicSafety.gc.ca

>>>>Government of Canada | Gouvernement du Canada

>>>>

>>>>

>>>>Need to report an incident? Find the Incident Report Form here:

>>>>

>>>>

>>>><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti>

>>>>/

>>>>i

>>>>t

>>>>imp

>>>>-pgimti-app-ann-D-eng.rtf

>>>>

>>>>Vous voulez rapporter un incident ? Utilisez le formulaire de

>>>>déclaration

>>>>suivant:

>>>>

>>>><http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti>

>>>>/

>>>>i

>>>>t
>>>>imp
>>>>-pgimti-app-ann-D-fra.rtf<<http://www.tbs-sct.gc.ca/sim-gsi/publicati>
>>>>o n s /do cs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fr.rtf>
>>>>
>>>>
>>>
>>
>

Breault, Stephen

From: [REDACTED]
Sent: Thursday, December 22, 2011 1:08 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: AC-2971 Potential Security Issue affecting [REDACTED]

Good day,

We would like to draw your attention to the following recent publication related to this issue. If you have any questions or comments, feel free to contact us.

Regards

Luc

URL: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

Content:
(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-003
Date: 20 December 2011

Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification

PURPOSE
=====

The goal of this Information Note is to raise awareness of a common but potentially insecure implementation of the PHP cURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (cURL or libcurl). The cURL library provides a set of functions that allows establishing connections using various communication protocols including HTTPS.

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Thursday, December 22, 2011 1:11 PM
To: [REDACTED]
Cc: CYBERDO
Subject: AC-2971 [REDACTED] security issue

Good day,

We would like to draw your attention to the following recent publication related to this issue. If you have any questions or comments, feel free to contact us.

Cheers

Luc

URL: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>
<<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>>

Content:

(La version française suit)

PUBLIC SAFETY CANADA

CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Government Operations Centre/

Centre des opérations du gouvernement

Email/courriel:

s.16(2)(c)

s.19(1)

s.20(1)(c)

Government Operations Centre/

Centre des opérations du gouvernement

Email/courriel:

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From:

Sent: November-15-11 11:08 PM
To: [REDACTED]
Subject: Re: AC-2971 [REDACTED] security issue

s.16(2)(c)

s.19(1)

s.20(1)(c)

Ignore that, I found the txt; I'm going to research it.

-j

On Tue, Nov 15, 2011 at 8:04 PM, [REDACTED] wrote:

Please resend the incident details; I never received them from you.

-j

On Tue, Nov 15, 2011 at 7:23 PM, [REDACTED]

[REDACTED] did you get the chance to look into this issue ? Would you have an update ?

Cheers

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 <tel:%2B1%20613-991-9949> Facsimile | Télécopieur +1 613-991-3574 <tel:%2B1%20613-991-3574> luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----

From: Beaudoin, Luc S
Sent: October 4, 2011 11:37 AM
To: [REDACTED]
Cc: Pitcher Robert
Subject: RE: [REDACTED] contact for unsecure api issue

Here are the details (attached).

We would appreciate your assessment of this information. Feel free to call me or Rob to discuss.

Thanks.

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 <tel:%2B1%20613-991-9949> Facsimile | Télécopieur +1 613-991-3574 <tel:%2B1%20613-
991-3574> luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Need to report an incident? Find the Incident Report Form here:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-eng.rtf>

Vous voulez rapporter un incident ? Utilisez le formulaire de déclaration suivant:

<http://www.tbs-sct.gc.ca/sim-gsi/publications/docs/2009/itimp-pgimti/itimp-pgimti-app-ann-D-fra.rtf>

-----Original Message-----

From: [REDACTED]
Sent: October 4, 2011 11:14 AM
To: Beaudoin, Luc S
Cc: Pitcher Robert
Subject: Re: [REDACTED] for unsecure api issue

s.16(2)(c)

s.19(1)

s.20(1)(c)

That key didn't paste well. Try this instead:



s.19(1)



s.16(2)(c)

s.19(1)

s.20(1)(c)

Breault, Stephen

From: [REDACTED]
Sent: Thursday, December 22, 2011 1:16 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: AC-2971 potential security issue in [REDACTED]

Bonjour, Good day,

We would like to draw your attention to the following recent publication related to this issue. If you have any questions or comments, feel free to contact us.

Cheers

Luc

URL: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

Content:
(La version française suit)

PUBLIC SAFETY CANADA
CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Number: IN11-003
Date: 20 December 2011

Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification

PURPOSE
=====

The goal of this Information Note is to raise awareness of a common but potentially insecure implementation of the PHP cURL option used to verify SSL certificates.

ASSESSMENT
=====

The PHP Hypertext Preprocessor is a flexible server-side scripting language. It allows developers to dynamically generate HTML pages. PHP implements a number of standard code libraries including Client URL (cURL or libcurl). The cURL library provides a set of functions that allows establishing connections using various communication protocols including HTTPS.

Centre des opérations du gouvernement
Email/courriel: [REDACTED]

s.16(2)(c)

s.19(1)

s.20(1)(c)

Government Operations Centre/
Centre des opérations du gouvernement
Email/courriel: [REDACTED]

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

-----Original Message-----

From: [REDACTED]
Sent: November-15-11 10:09 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE:AC-2971 potential security issue in [REDACTED]

Bonjour, Good day,

Have you had a chance to look into this potential issue ? Here are some additional details:

Modules potentially affected:

[REDACTED]

Code:

[REDACTED]

Other similar modules:

[REDACTED]



Other packages have acknowledge this issue and issued updates accordingly.

s.16(2)(c)

s.19(1)

Luc

s.20(1)(c)

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----

From: Beaudoin, Luc S

Sent: October 26, 2011 2:32 PM

To: [REDACTED]

Subject: RE: potential security issue in [REDACTED]

We were informed of the way osCommerce uses PHP cURL to verify SSL certificate in various modules which may be unsecured due to the VERIFYPEER option being set to False by default.

We would like to raise awareness of this coding practice amongst key ecommerce package development community to avoid server-to-server communications being potentially vulnerable to m-i-m attacks.

I have specifics on some of the modules this may affect, but I would like to know what your thoughts are on this, and if you have a PGP key.

Luc

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

-----Original Message-----

From: [REDACTED]
Sent: October 26, 2011 2:24 PM
To: Beaudoin, Luc S
Subject: Re: potential security issue in osCommerce

Hi Luc..

Please tell me what you have discovered.

Kind regards,

[REDACTED]

On Wed, Oct 26, 2011 at 7:43 PM, Beaudoin, Luc S <Luc.Beaudoin@ps-sp.gc.ca> wrote:

> Good day,
>
> Could you assist us with identifying the best mechanism/contact to
> bring forward a potential security issue in [REDACTED] code ?
>
>
> Luc Beaudoin, P.Eng, MSc, MBA
> Chief Cyber Operations | Chef des opérations cybernétiques Canadian
> Cyber Incident Response Centre | Centre canadien de réponse aux
> incidents cybernétiques Public Safety Canada | Sécurité publique
> Canada Telephone | Téléphone +1 613-991-9949 Facsimile | Télécopieur
> +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca Government
> of Canada | Gouvernement du Canada
>
>
>

Breault, Stephen

From: [redacted]
Sent: Thursday, December 22, 2011 1:18 PM
To: [redacted]
Cc: 'security'
Subject: AC-2971: Potential Security Issue [redacted]

Good day [redacted]

We would like to draw your attention to the following recent publication related to this issue. If you have any questions or comments, feel free to contact us.

Cheers

Luc

URL: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>
<<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>>

Content:

(La version française suit)

PUBLIC SAFETY CANADA

CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

Téléphone : 613-944-4875 ou 1-800-830-3118 Télécopieur : 613-998-9589 Courriel : communications@ps-sp.gc.ca
<<mailto:communications@ps-sp.gc.ca>>

s.16(2)(c)

s.19(1)

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

s.20(1)(c)

Government Operations Centre/

Centre des opérations du gouvernement

Email/courriel:

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: Beaudoin, Luc S

Sent: November-15-11 9:53 PM

To: [REDACTED]

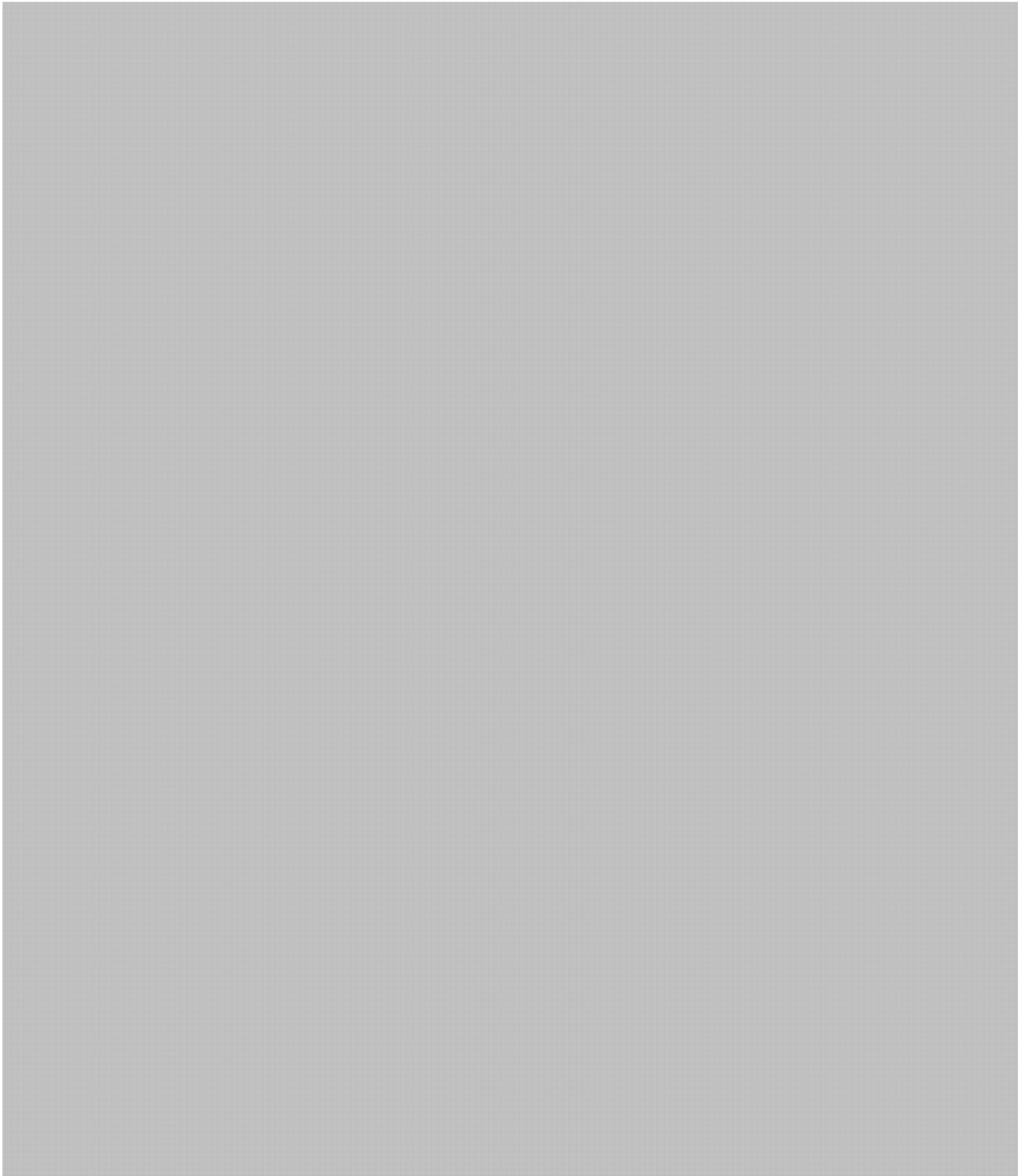
Cc: security

Subject: RE: Potential Security Issue [REDACTED]

Hi [REDACTED] have you had the chance to look into this potential issue ? here are the specifics:

The following modules seem to not perform SSL certificate verification based on their cURL VERIFYPEER setting.

[REDACTED]



Other packages have acknowledge this issue and addressed it in new version.

Let me know. Tx!

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

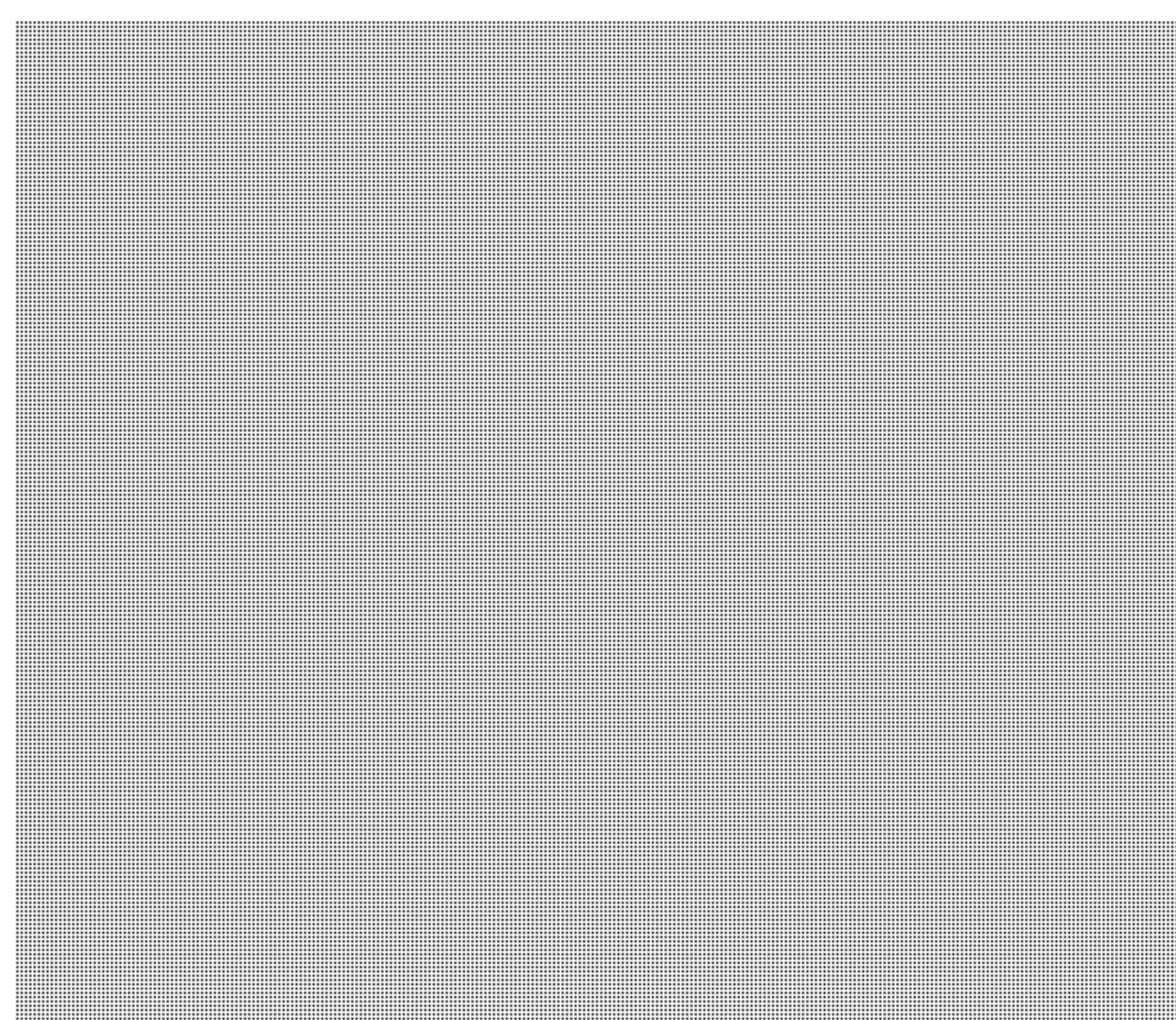
From: [REDACTED]
Sent: October 26, 2011 2:54 PM
To: Beaudoin, Luc S
Cc: security
Subject: RE: Potential Security Issue with [REDACTED]

Thanks Luc,

We'll have the team check it out, and I'll get back to you with any information as soon as it is available. Thank you for reporting this directly to us. We'll keep you posted.

Feel free to contact me if you have any questions.

Regards,



s.16(2)(c)

s.19(1)

s.20(1)(c)

email

tel

fax

From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]

Sent: Wednesday, October 26, 2011 11:49 AM

To: [REDACTED]

Subject: RE: Potential Security Issue with Magento

Thanks [REDACTED]

A researcher reported to us a potential security issue which has to do with the use of PHP cURL in various modules of [REDACTED]. Specifically, some modules seem to use the VERIFYPEER option set to False by default, or may otherwise fail to properly validate the SSL certificate. This may result in unsecured channels between web-applications and information processing services.

We would like to raise awareness of this coding practice amongst key ecommerce package development community to avoid server-to-server communications being potentially vulnerable to m-i-m attacks.

I have specifics on some of the modules this may affect, but I would like to know if you were aware of this potential issue and what your thoughts may be about its significance.

Luc

s.16(2)(c)

s.19(1)

s.20(1)(c)

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: [REDACTED]
Sent: October 26, 2011 2:43 PM
To: Beaudoin, Luc S
Cc: security
Subject: RE: Potential Security Issue [REDACTED]

Hi Luc,

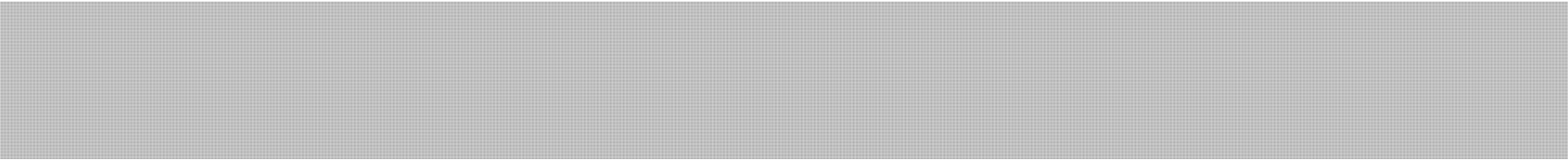
This is the best channel.

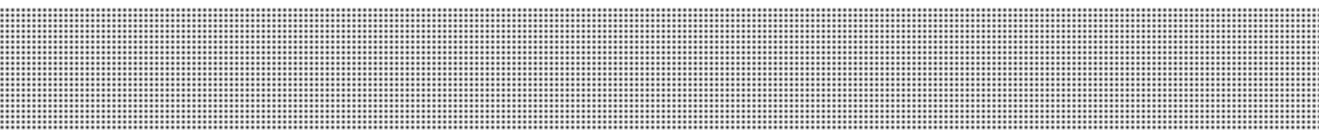
Regards,

Rhonda

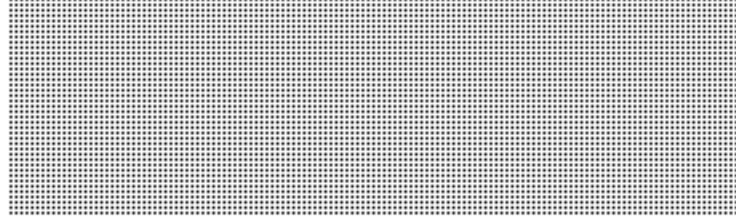
email [REDACTED]

tel [REDACTED]
fax [REDACTED]



From: Beaudoin, Luc S [mailto:Luc.Beaudoin@ps-sp.gc.ca]
Sent: Wednesday, October 26, 2011 11:38 AM
To: 
Subject: Potential Security Issue with Magento
Importance: High

Good day,

Could you assist us with identifying the best mechanism/contact to bring forward a potential security issue 
code ?

Thank you

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Breault, Stephen

From: [REDACTED]
Sent: Thursday, December 22, 2011 1:22 PM
To: [REDACTED]
Subject: AC-2971: [REDACTED]

Good day [REDACTED]

We would like to draw your attention to the following recent publication related to this issue. If you have any questions or comments, feel free to contact us.

Cheers

Luc

URL: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>
<<http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>>

Content:

(La version française suit)

PUBLIC SAFETY CANADA

CANADIAN CYBER INCIDENT RESPONSE CENTRE

INFORMATION NOTE

En cas de questions urgentes, ou pour signaler des incidents, veuillez communiquer avec le COG.

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

s.16(2)(c)

s.19(1)

s.20(1)(c)

From: Beaudoin, Luc S

Sent: October-26-11 3:20 PM

To: [REDACTED]

Subject: RE: [REDACTED]

We will. thanks. The issue had to do with the default setting of the PHP cURL VERIFYPEER option in various payment modules. This option appears to be set to false, which could result in unvalidated SSL connections.

Luc

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<mailto:luc.beaudoin@ps-sp.gc.ca> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

s.16(2)(c)

s.19(1)

s.20(1)(c)

From: [REDACTED]

Sent: October 26, 2011 3:03 PM

To: Beaudoin, Luc S

Subject: Re: [REDACTED]

[REDACTED]

can you please ensure that the security issue is on the latest version of the [REDACTED]

thanx

[REDACTED]

On 10/26/11 2:24 PM, Beaudoin, Luc S wrote:

Good day,

Could you provide us with a contact/mechanism to communicate a potential security issue reported to us potentially

[REDACTED]

thanks

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

Telephone | Téléphone +1 613-991-9949

Facsimile | Télécopieur +1 613-991-3574

luc.beaudoin@ps-sp.gc.ca <mailto:luc.beaudoin@ps-sp.gc.ca>

PublicSafety.gc.ca

Government of Canada | Gouvernement du Canada

Breault, Stephen

From: Mail Delivery System <MAILER-DAEMON@scmze026.ssan.egs-seg.gc.ca>
To: [REDACTED]
Sent: Thursday, December 22, 2011 1:23 PM
Subject: Undeliverable: AC-2971: Potential Security Issue [REDACTED]

Delivery has failed to these recipients or groups:

[REDACTED]
A problem occurred during the delivery of this message to this e-mail address. Try sending this message again. If the problem continues, please contact your helpdesk.

The following organization rejected your message: [REDACTED]

Diagnostic information for administrators:

Generating server: scmze026.ssan.egs-seg.gc.ca

Original message headers:

Received: from unknown (HELO scmze000.ssan.egs-seg.gc.ca) [REDACTED] by
inbound.ssan.egs-seg.gc.ca with ESMTP; 22 Dec 2011 17:53:16 +0000
Received: from ns.ps-sp.gc.ca (HELO mail.ps-sp.gc.ca) ([REDACTED] by
scmze000.ssan.egs-seg.gc.ca with ESMTP; 22 Dec 2011 18:01:39 +0000
From: [REDACTED]
To: [REDACTED]
CC: [REDACTED]
Subject: AC-2971: Potential Security Issue [REDACTED]
Thread-Topic: AC-2971: Potential Security Issue [REDACTED]
Thread-Index: AczA1fTbCQvJqiBuRTCmrgB66owDMQ==
Date: Thu, 22 Dec 2011 18:18:23 +0000
Message-ID: <39BA97E7DB50A3458A74DC5F428F4A94048FAF54@PENCR03.PSEPC-SPPCC.NET>
Accept-Language: en-CA, en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:

s.16(2)(c)

Content-Type: text/plain
MIME-Version: 1.0



AC-2971:
Potential Securit...

Breault, Stephen

From: Beaudoin, Luc S
Sent: Friday, December 23, 2011 2:40 PM
To: Anderson, Windy; Dick, Robert
Subject: cURL Media Line Draft. Take 2

1. The cURL library is a very popular and open source software tool used to establish an internet connection between two computers. This software can be used for secured connections as well. CCIRC was informed that in some cases where secured connections are expected, like for transactions processing or critical infrastructure applications, the cURL tool may not be implemented properly. Such faulty implementations could expose secured data if a malicious individual managed to intercept it.
2. The CCIRC worked with a number of organisations to confirm the issue and implement mitigations where appropriate.
3. The CCIRC posted IN11-003 on the Public Safety website to promote appropriate use of this tool in secure applications.

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

From: Beaudoin, Luc S
Sent: December-23-11 1:19 PM
To: Anderson, Windy; Dick, Robert
Subject: cURL Media Line Draft. Take 1

1. The Information Note raises awareness of a potentially common insecure coding practice in web applications. It describes how a specific tool often used by internet applications, cURL, may not always be used with all its security features properly enabled. In this case, the security feature CCIRC is concerned with involves the verification mechanism used to confirm that a remote computer system is the actual valid one. This can be done using cryptologically verified certificates. In some applications requiring enhanced security, like transactions processing or critical infrastructure applications, the verification of the remote host authenticity may be very important.
2. The CCIRC worked with the Canadian researcher Kevin McArthur and CIPPIC to confirm the issue and provide this public product with advice on how to determine if one's web application is properly implemented and how it may be

resolved otherwise. CCIRC also directly contacted various web application and software package providers to raise their awareness of this potential issue and implement mitigations where appropriate.

3. Specifically, CCIRC chose to post this product on its website to reach out to as many software developers and website operators as possible who potentially use this technology and encourage them to consider the provided recommendations.

Luc Beaudoin, P.Eng, MSc, MBA

Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada

Breault, Stephen

From: Dick, Robert
Sent: Thursday, December 29, 2011 9:46 AM
To: Beaudoin, Luc S
Subject: Re: FYI Follow-up questions on CCIRC Notice

The reporter wants the names of all companies with whom ccirc partners and shares info -- and we don't share that as a matter of privacy.

From: Beaudoin, Luc S
Sent: Thursday, December 29, 2011 09:28 AM
To: Dick, Robert
Subject: Re: FYI Follow-up questions on CCIRC Notice

Quick comment: The appropriateness of disclosing the companies name is debatable. DHS - US CERT, and many other CERTs, routinely do it. This is one of the difficult functions of a CERT: using public disclosure as a lever to obtain timely mitigation of vulnerabilities.

Luc Beaudoin
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca PublicSafety.gc.ca
Government of Canada | Gouvernement du Canada

Sent from a mobile device | Envoyé d'un appareil portable

From: Dick, Robert
Sent: Thursday, December 29, 2011 09:14 AM
To: Slack, Jessica
Cc: Labelle, Sébastien; Anderson, Windy; Beaudoin, Luc S; Bendelier, Kenneth; Hatfield, Adam; Gordon, Robert
Subject: Re: FYI Follow-up questions on CCIRC Notice

Thx.

From: Slack, Jessica
Sent: Thursday, December 29, 2011 09:11 AM
To: Dick, Robert
Cc: Philipps, Lisa
Subject: FYI Follow-up questions on CCIRC Notice

Hi Robert...just fyi. Here is the response that MO just approved.

Pages 422 to / à 438

are duplicates

sont des duplicatas

Pages 422 to / à 438

are duplicates

sont des duplicatas

Pages 422 to / à 438

are duplicates

sont des duplicatas



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

Table of Contents

Incident reporting.....	1
1. CE11-2549 [Stratfor Hack affected Canadians]	1
2. CE11-2554 [Sinkhole Notification – Multiple Organizations]	1
3. CE12-2559 [Sinkhole Notifications - Multiple Organizations]	1
4. CE12-2565 [Shadowserver Drone Notifications - Multiple Organizations].....	1
Financial Sector.....	2
1. CE11-2545 [Shaw Phishing email].....	2
2. CE11-2547 [Scotiabank Phishing].....	2
3. CE11-2550 [BMO Phishing]	2
4. CE11-2552 [RBC Phishing]	2
5. CE11-2553 [TD Canada Trust Phishing].....	2
6. CE12-2556 [Visa Phishing]	2
7. CE12-2557 [RBC Phishing]	2
8. CE12-2558 [RBC Phishing]	3
9. CE12-2562 [BMO Phishing]	3
10. CE11-2564 [RBC Phishing]	3
Federal Government.....	3
1. CE11-2548 [Federal Department vulnerable to XSS].....	3
Provincial Government	3
1. CE11-2551 [Sinkhole Notification – Provincial Government].....	3
Electrical and Energy	3
Telecommunication Sector.....	3
1. CE12-2555 [Defacement hosting provider website].....	3
Academia/Universities	4
1. CE12-2563 [University website defacement]	4
Other Organizations	4
1. CE12-2561 [Building Control System Login Screen Web Exposed]	4
Partners.....	5
Watch List	5
Malware Indicators.....	5
1. CVE-2010-3333 related exploit delivered through phishing emails:.....	5
2. Network Security and government notifications related targeted phishing emails:.....	6
3. Other targeted attacks and spear phishing trojanised file indicators:.....	6
4. Lilupophilupop SQL Injections	6
CCIRC Cyber Awareness Products.....	7
Alert	7
1. AL11-005 Hash Table Implementations Vulnerable to Attack.....	7
Advisories	7
1. AV11-051 Microsoft Out-of-Band Security Bulletin	7
Information Notes	7
1. IN11-003 Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification.....	7
Technical Reports.....	7
Cyber Flashes	7
Threat and Vulnerability Monitoring	7
Vulnerabilities:.....	8



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

1.	Microsoft Windows win32k.sys Memory Corruption Vulnerability	8
2.	Microsoft Windows Phone DoS	8
3.	Microsoft Office Graph DataFormat Signed Index Code Execution Vulnerability (MS11-072)	8
4.	OpenSSL Multiple Vulnerabilities.....	8
5.	Apache Struts Multiple Vulnerabilities.....	8
6.	Certain HP LaserJet Printers, Remote Unauthorized Access to Files.....	8
7.	IBM WebSphere Application Server Community Edition Tomcat Container Denial of Service.....	9
	Threat Watch:.....	9
1.	Gameover' Delivered Via Phishing E-Mails	9
2.	Spam Emails Link To QR Codes.....	9
	Malware and SPAM Reports.....	9
	Publicly Reported Compromises.....	9
1.	U.S. Chamber of Commerce details 'sophisticated' 6-month hacking of its computers. ..	9
2.	Chinese Internet Suffers the Most Serious User Data Leak in History.....	10
3.	Symantec's Norton AntiVirus source code exposed by hackers	10
4.	Sony Pictures Website and Facebook Page Hacked by Anonymous.....	10
	SCADA/ICS.....	10
1.	ICSA-12-006-01—3S SMART SOFTWARE SOLUTIONS CODESYS VULNERABILITIES	11
2.	ICSA-11-343-01—SIEMENS FACTORYLINK MULTIPLE ACTIVEX VULNERABILITIES	11
3.	ICSA-11-332-01A—INVENSYS WONDERWARE INBATCH ACTIVEX VULNERABILITIES	11
4.	ICSA-11-362-01—SCADATEC SCADAPHONE/MODBUS TAGSERVER BUFFER OVERFLOW.....	11
5.	ICSA-11-298-01A—SIELCO SYSTEMI WINLOG BUFFER OVERFLOW	11
6.	ICSB-11-327-01—ILLINOIS WATER PUMP FAILURE REPORT.....	11
7.	ICSA-11-361-01— SIEMENS AUTOMATION LICENSE MANAGER MULTIPLE VULNERABILITIES	11
8.	ICSA-11-356-01 - Siemens SIMATIC HMI Authentication Vulnerabilities	11
9.	ICSA-11-355-02 - WellinTech KingView Buffer Overflow	11
10.	ICSA-11-355-01 - 7-Technologies IGSS Buffer Overflow Vulnerability.....	11
	Noteworthy News.....	12
5.	Canada Post is warning its customers that a circulating email that claims price discrepancies between corporate and private postal outlets is fake.....	12
6.	Exploit Kits Now Updated With New Wares Before Patches Are Ready	12
7.	Critical holes in Firefox, Thunderbird and SeaMonkey.....	12
8.	Anonymous aims to make US Senators accountable for their votes.....	13
9.	Microsoft confirms Windows vulnerability "Microsoft has posted on its German language	13
10.	New Facebook clickjacking scam spreads like fire	13
11.	Team Black Hat gave warning to Anonymous	14
12.	Anti-spam plan lacks teeth: prof.....	14



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

s.16(2)(c)

Incident reporting

This section contains information related to incidents affecting Critical Infrastructure in Canada.

1. CE11-2549 [Stratfor Hack affected Canadians]

CCIRC received a report from law enforcement community about a hack of Stratfor by Anonymous. The link to information initially posted on Pastebin is: [REDACTED]

STRATFOR's client list including emails, passwords, home/office addresses and credit card information were posted publically. This event is quite extensive as approximately 75,000 credit card numbers and 860,000 login credentials have been compromised.

Stratfor sent a notification email to all its clients.

CCIRC recommendations:

- 1) Financial Risk: credit card information posted online contained the full 16 digit number, expiry date, and CVV number. Individuals should contact their bank and advise them of this incident. The bank will help set up any counter-measures for that individuals card.
- 2) Targeted Attacks: Compromised individuals could become victims of specific and targeted attacks, such as malicious emails, social engineering, and attempts to compromise workplace security. Request that individuals change the password of all other accounts, (business or personal on the Internet), that use elements from the compromised password. Request the individual contact their IT Security if they believe they are being targeted with suspicious emails.
- 3) Privacy Information: Impacted individuals privacy could be compromised. Work and home telephone numbers and addresses were potentially released. Individuals should be aware this information has been made public and to be diligent when responding to enquiries over the telephone.

Thousands of Canadians were affected by this breach. CCIRC notified federal and provincial organisations affected based on available data.

2. CE11-2554 [Sinkhole Notification – Multiple Organizations]

Sinkhole notifications for data available on the 29 Dec to multiple organizations in various critical infrastructure sectors. Hosts within these organizations may be affected by DNS Changer malware.

DNS Changer malware is affecting over 19 000 Canadian computers at the moment.

3. CE12-2559 [Sinkhole Notifications - Multiple Organizations]

Sinkhole notifications for data available on the 3 Jan to multiple organizations in various critical infrastructure sectors. Hosts within these organizations were communicating with a sinkhole server. Infection types included DNS Changer, Mebroot, and Torpig.

4. CE12-2565 [Shadowserver Drone Notifications - Multiple Organizations]

Sinkhole notifications for data available on the 8 Jan to multiple organizations in various critical infrastructure sectors. Hosts within these organizations were communicating with a sinkhole server. Infection types included: Artro, DNS Changer, GBot, SpyEye, Carberp and Zeus.



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

Financial Sector

1. CE11-2545 [Shaw Phishing email]

hxxps://docs[.]google[.]com/spreadsheet/viewform?formkey=dFFhUW5WWHdBu2ZfdWNOa0g3M2lqT3c6MQ
(Google Docs hosting services)

2. CE11-2547 [Scotiabank Phishing]

hxxp://erdireklam[.]hu/scotiaonline ip address is 87.229.26.126 ASN 29278 (Hungary, HU)

3. CE11-2550 [BMO Phishing]

hxxp://abzug[.]ch/templates/beeze/images_general/UpdatedBMO[.]html
(80.74.142.130 - METANET GmbH, Switzerland)

4. CE11-2552 [RBC Phishing]

hxxp://bilingualfreeschool[.]co[.]uk/css/form/
62.193.220.178 (AMEN Networks, Paris France)

5. CE11-2553 [TD Canada Trust Phishing]

hxxp://ldfaerch[.]com/images/accueil/
46.105.227.9 (OVH ISP Paris France)
This site redirected to the final phishing page located at:
hxxp://www[.]wslytyler[.]org/css/easywebsoc/
74.124.10.26 (EBL Global Network, Dallas Texas)

6. CE12-2556 [Visa Phishing]

hxxp://charltonhats[.]com/admin[.]html
63.247.80.138(Global Net Access – Atlanta Georgia).
This site redirected to the final phishing page located at:
hxxp://downeastenterprises[.]com/update/update[.]jsp/visavoorjou/info/cgi-
login/00D02D002A00D02100DA0G0QF92120202910010201003S1123331/
on the same server (63.247.80.138)

7. CE12-2557 [RBC Phishing]

hxxp://malakao[.]es/feed/rss
91.142.209.115 (Axarnet Communications – Malaga Spain)



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

8. CE12-2558 [RBC Phishing]

hxxp://vdz-599196[.]amen-pro.com/css/form/
62.193.220.178 (AMEN Networks, Paris France)

9. CE12-2562 [BMO Phishing]

hxxp: //rhiotap[.]net/wso2/mt/cgi-bin/
208.116.35.238 (Fortress ITX Clifton New Jersey)

10. CE11-2564 [RBC Phishing]

hxxp://blog[.]kennysells[.]com/wp-includes/www1[.]royalbank[.]com/cgi-
bin/rbaccess/rbunxcgi[.]htm?F6=1&F7=IB&F21=IB&F22=IB&REQUEST=ClientSignin&LAN
GUAGE=ENGLISH
173.236.203.142 (New Dream Network, Brea California)

Federal Government

1. CE11-2548 [Federal Department vulnerable to XSS]

CCIRC sent notification to CTEC for evaluation and notification of a potentially vulnerable federal website.

Provincial Government

1. CE11-2551 [Sinkhole Notification – Provincial Government]

Sinkhole notifications for data available on the 28 Dec to multiple provincial organizations. Hosts within these organizations may be affected by Mebroot.

Electrical and Energy

NIL

Telecommunication Sector

1. CE12-2555 [Defacement hosting provider website]

CCIRC observed that a website operated by an Internet hosting service provider located in Manitoba was recently defaced. Notification sent to the hosting provider.

CCIRC recommendations:

- * Check web server logs for any indication of unusual activity against your website or supporting databases.
- * Change administrator and FTP passwords for the server/website.
- * Check for any new user accounts with admin privileges that may have been recently created.



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

Academia/Universities

1. CE12-2563 [University website defacement]

CCIRC observed that a website registered to a university was recently defaced. Notification sent to the university.

CCIRC recommendations:

- * Check web server logs for any indication of unusual activity against your website or supporting databases.
- * Change administrator and FTP passwords for the server/website.
- * Check for any new user accounts with admin privileges that may have been recently created

s.16(2)(c)

Other Organizations

s.20(1)(c)

1. CE12-2561 [Building Control System Login Screen Web Exposed]

A post to Twitter disclosed the log-in screen for the building control system of a public building in Ontario.

Twitter Post:

The building is managed by [REDACTED] a control system service company

CCIRC contacted [REDACTED] and spoke with their Operations Manager.

CCIRC informed [REDACTED] of the posting on Twitter and outlined our concerns as a result of this action. Mitigations were implemented. CCIRC recommendations:

- * The administrator responsible for the system should ensure that a strong password is used and not one that is default or easily guessed.
- * change the log-in screen banner to a more generic title so that who and where the system is located was not obvious.
- * Ensure the system running this service is fully patched. Review firewall rules and services such as ftp to ensure these services are well locked down to prevent unauthorized access to control systems.



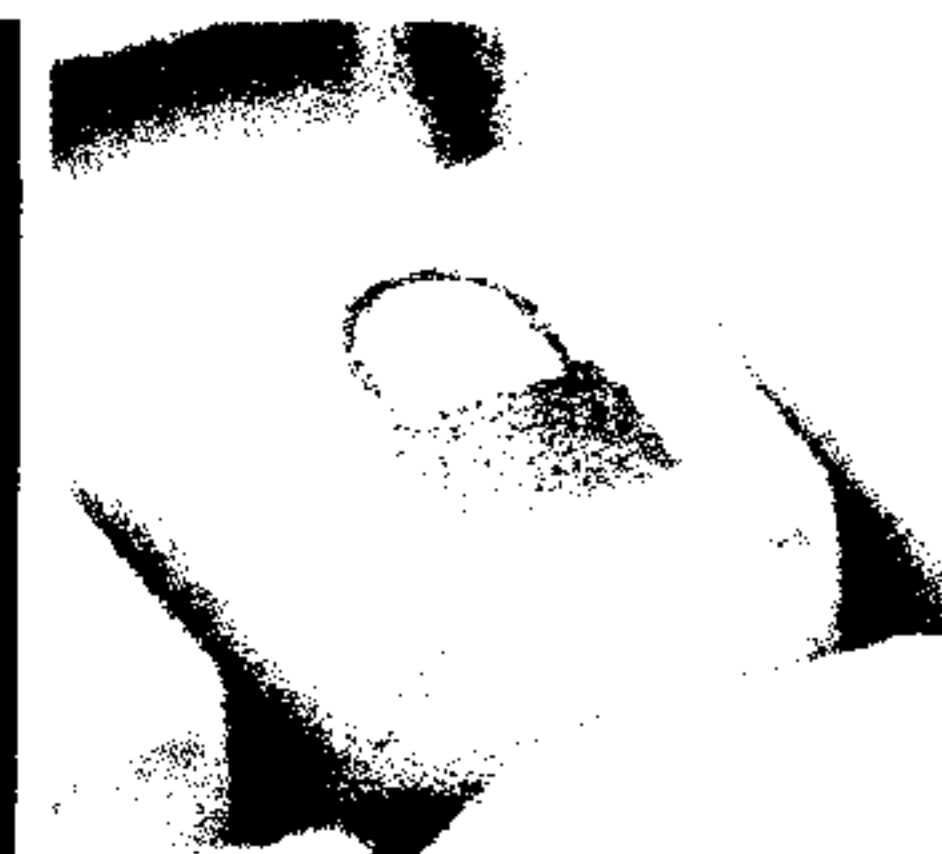
Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

OPERATIONAL SUMMARY CCIRC Cyber Awareness Product



Weekly Technical Report

Issued: 11-Jan-2012

Volume 2012 - 01

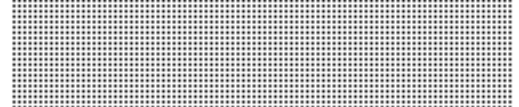
DISCLAIMER

This publication is **UNCLASSIFIED - For Official Use Only** and is the property of Public Safety Canada. Prepared by the CCIRC, it is derived from various sources with information effective as of the date of publication and provided to your agency/department in confidence. This document must not be reclassified or disseminated, in any way, in whole or in part, without the consent of the originator. The information contained in this message is provided strictly for the purpose of defensive reconfiguration of assets owned by the recipient. The recipient shall not engage in any form of information collection activities outside its own network perimeter using the information within this product. Such actions include probing, downloading, browsing or crawling sites contained within this report.

CCIRC Cyber Awareness Products (CCAPs) are organized into the following categories:

- **Flash:** Perceived threat and/or vulnerability; No patch available
- **Advisory:** Threat present affecting Canadian national infrastructure; Patches available
(Advisories and Flash marked URGENT indicate an immediate/emerging threat against the Canadian national Infrastructure; Action required)
- **Report:** Strategic, Information, or Technical
- **Operational Summary:** Daily, Weekly, Monthly

NOTE TO READERS

CCAPs are available at the following website: <http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx>. If you have any questions, please contact the Public Safety Cyber Duty Officer @ 

s.16(2)(c)

Traffic Light Protocol: RED: Designated for a specific audience/Non-sharable
AMBER: Sharable within organization on a need-to-know basis/Non-publishable
GREEN: Sharable within organization or community/Non-publishable
WHITE: Free to distribute



Partners

Watch List

Watch List associated with malicious activity in the last period. This is not a block list and CCIRC recommends using the list as indicators only over the last 7 days prior to 4 January 2012.

ip

country

s.16(2)(c)

Malware Indicators

1. CVE-2010-3333 related exploit delivered through phishing emails:

File name:

Malware:

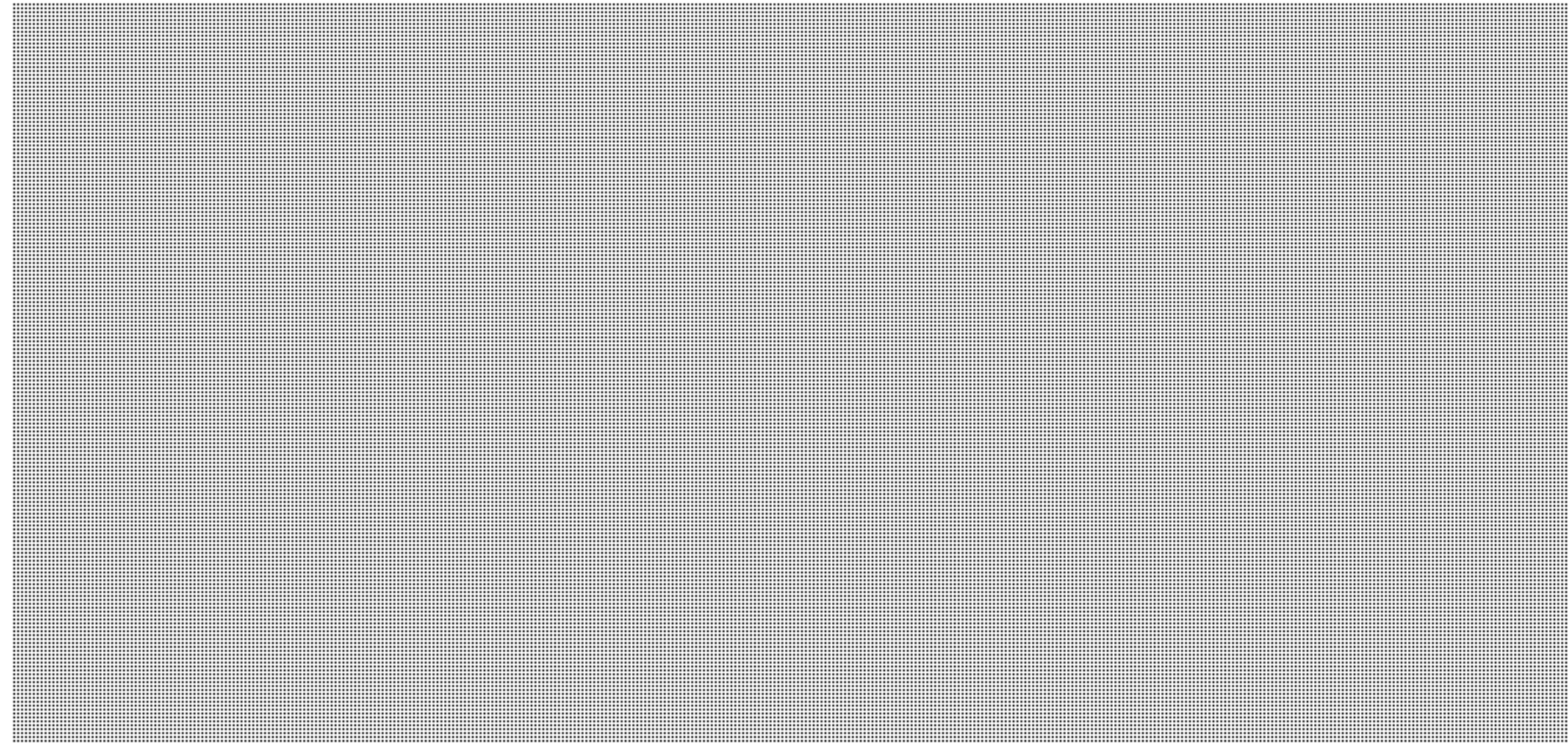
Related Indicators:

s.16(2)(c)

Public Safety
CanadaSécurité publique
Canada

TLP: AMBER

Canada



Reference:

<http://www.threatexpert.com/report.aspx?md5=65b654ea065dadd88dd1b686c0628943><http://xml.ssdsandbox.net/view/f76b95bcf542ae6f49fc820328b13f9a>

2. Network Security and government notifications related targeted phishing emails:

Malware: Zeus ICEIX

Command and Control:

(https://zeustracker.abuse.ch/monitor.php?host=plantlunch.ru&id=5d24056d985d594f25b955348d9c4a60)

Dropper:

Email sample:

Subject:

From (spoofed):

3. Other targeted attacks and spear phishing trojanised file indicators:

*Note:

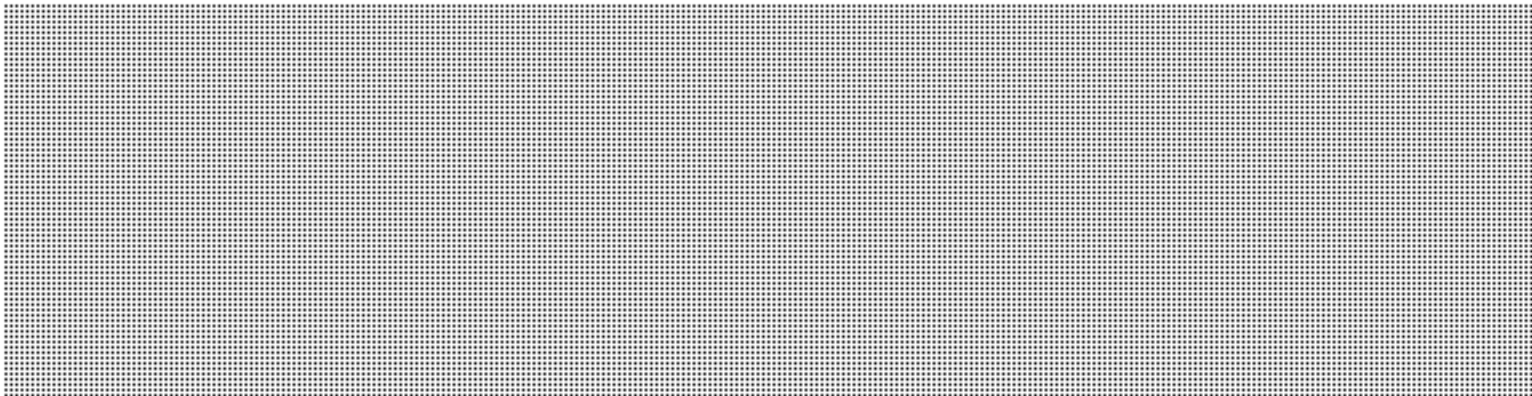
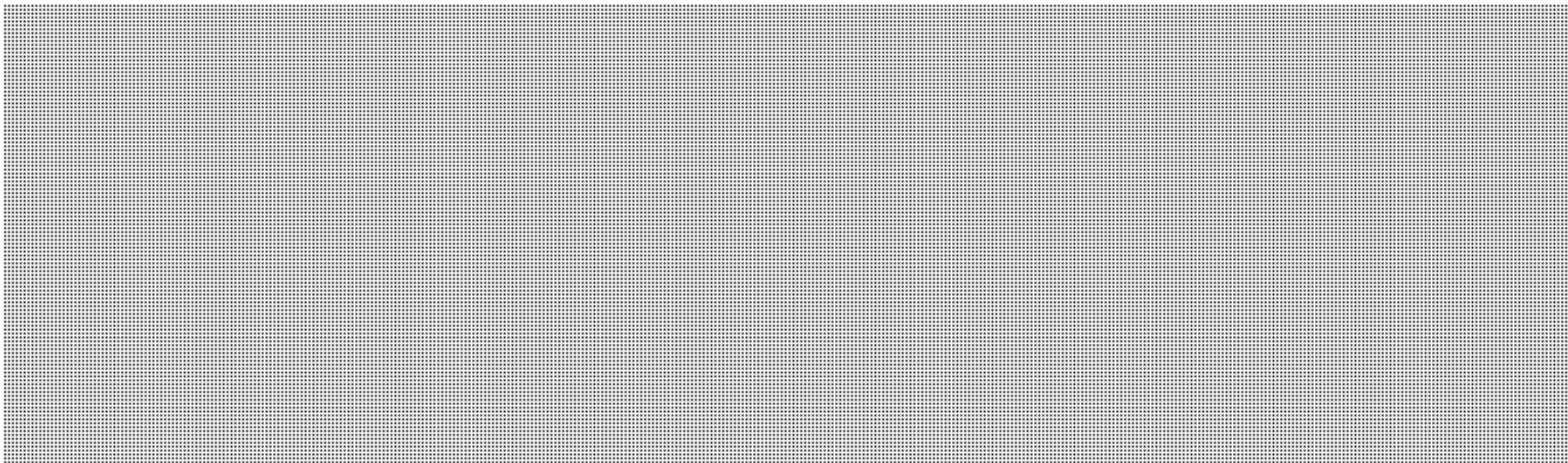
*These are Lurid related

4. Lilupophilupop SQL Injections

Public Safety
CanadaSécurité publique
Canada

TLP: AMBER

Canada


Associated domains:


CCIRC Cyber Awareness Products

Alert

1. AL11-005 Hash Table Implementations Vulnerable to Attack

Link: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/al11-005-eng.aspx>

Advisories

1. AV11-051 Microsoft Out-of-Band Security Bulletin

Link: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/av11-051-eng.aspx>

Information Notes

1. IN11-003 Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification

Link: <http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-003-eng.aspx>

Technical Reports

NIL

Cyber Flashes

NIL

Threat and Vulnerability Monitoring

This section contains threats and vulnerabilities that did not meet the publication criteria for CCIRC products other than operational summaries. It is not meant to be an exhaustive list but rather a heads-up on potentially significant threats and vulnerabilities affecting technologies available to CCIRC communities of interest.



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

Vulnerabilities:

1. Microsoft Windows win32k.sys Memory Corruption Vulnerability

While using the Apple Safari browser, a user visiting a crafted page that includes an IFRAME containing a large height attribute, it can allow for remote code execution with kernel-mode privileges. It has been confirmed and the vulnerability exists on a fully patched WIN 7/64 OS. NO CVE. No patch available.

- Reference: <http://secunia.com/advisories/47237/>

2. Microsoft Windows Phone DoS

By sending a crafted SMS, Windows Messenger or Facebook Chat message it can trigger a reboot of the unit and render all messaging unusable. Microsoft is currently testing a fix. NO CVE

- Reference: <http://secunia.com/advisories/47256/>

3. Microsoft Office Graph DataFormat Signed Index Code Execution Vulnerability (MS11-072)

By getting the user to open a malicious file or web page containing an Excel or PowerPoint graph the malicious user can exploit an out-of-bound index error to run remote code with the application's permission level. This has been confirmed in Microsoft Office 2007+. This is an old vulnerability but it has been found to be exploited in a few cases. (Victims were not identified). CVE-2011-1990

- Reference: <http://www.securiteam.com/windowsntfocus/5ZP300U60U.html>

4. OpenSSL Multiple Vulnerabilities

They have released cumulative advisory urging users to upgrade to OpenSSL 1.0.0f or 0.9.8s. The patch addresses CVE-2011-4108,4109,4576,4577,4619,0027

- Reference: <http://secunia.com/advisories/47426/>

5. Apache Struts Multiple Vulnerabilities

These vulnerabilities exist in various modules on the server including input sanitization class, cookieInterceptor class and the ParameterInterceptor class. These can be used to execute code on the server from a remote location. NO CVE. A patch is available.

- Reference: <http://secunia.com/advisories/47393/>

6. Certain HP LaserJet Printers, Remote Unauthorized Access to Files

An undisclosed flaw in the firmware on some HP Laserjet Printers allows remote users to view files queued for printing. NO CVE but CVSS 7.9. Vendor patch available.

- Reference:

http://h20565.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c03140700&ac.admitted=1326200013725.876444892.492883150



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

7. IBM WebSphere Application Server Community Edition Tomcat Container Denial of Service

It can be exploited by sending a remote request with a considerably long list of parameters. NO CVE. A vendor patch is available.

- Reference: <http://secunia.com/advisories/47473/>

Threat Watch:

1. Gameover' Delivered Via Phishing E-Mails

The malware steals credentials and defeats common methods of user authentication employed by financial institutions. This is a new variant of the Zeus malware.

- Reference: http://www.fbi.gov/news/stories/2012/january/malware_010612/malware_010612

2. Spam Emails Link To QR Codes

They look like traditional spam messages but provide a picture of a QR code. There is no way to know where the code will lead allowing the spammers to redirect the users to any site on their mobile device. This could potentially be used to link to malware for the mobile devices/

- Reference: <http://community.websense.com/blogs/securitylabs/>

Malware and SPAM Reports

NIL

Publicly Reported Compromises

1. U.S. Chamber of Commerce details 'sophisticated' 6-month hacking of its computers.

Hackers in China spent at least six months inside the computers of the U.S. Chamber of Commerce and can still break in despite a massive security update, the lobby group said Wednesday. The Chamber, which lobbies on behalf of almost all major U.S. corporations, described a "sophisticated" hacker attack. "This was clearly somebody very sophisticated, who knew exactly who we are and who targeted specific people and used sophisticated tools to try to gather intelligence," said David Chavern, chief operating officer of the Chamber. The Wall Street Journal originally reported the security breach and said four Asia specialists at the 3-million-member Chamber were targets. At a daily news briefing in Beijing, foreign minister spokesman Liu Weimin called the report and the Chamber's response "baseless whipping up of so-called hacking. Chinese law bans hacking," Reuters News Agency reported.

- Reference: <http://www.thestar.com/news/article/1105272>



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

2. Chinese Internet Suffers the Most Serious User Data Leak in History

China's largest software programmers' Web site CSDN (China Software Developer Network) was hacked, and account information for more than 6 million users was leaked and quickly spread via the Internet. This incident is the largest data leak ever in China. The public databases contained personal account information, including user names, passwords, and email addresses. This data leak has caused great concern among millions of Chinese "netizens," especially those who use the same user name and password to access multiple Web sites. Clearly, this practice increases risk for these users, as criminals can easily use information from 1 account to log in to a user's other accounts to obtain even banking information. The root cause and scale of the leaks are still under investigation.

- Reference: <http://community.websense.com/blogs/securitylabs/archive/2011/12/27/chinese-internet-suffered-the-most-serious-user-s-data-leakage-in-history.aspx>

3. Symantec's Norton AntiVirus source code exposed by hackers

Symantec, the makers of Norton AntiVirus, has confirmed that a hacking group has gained access to some of the security product's source code. They release a statement: "Symantec can confirm that a segment of its source code has been accessed. Symantec's own network was not breached, but rather that of a third party entity. We are still gathering information on the details and are not in a position to provide specifics on the third party involved. Presently, we have no indication that the code disclosure impacts the functionality or security of Symantec's solutions. Furthermore, there are no indications that customer information has been impacted or exposed at this time."

- Reference: <http://nakedsecurity.sophos.com/2012/01/06/symantec-norton-antivirus-source-code-hackers/>

4. Sony Pictures Website and Facebook Page Hacked by Anonymous

After Sony has declared their support for the Stop Online Piracy Act (SOPA) a hacker that claims to be part of Anonymous allegedly breached the website of Sony Pictures and also managed to take over their Facebook profile. The cybercriminals called S3rver.exe, Anonnerd and N3m35151 even posted a couple of YouTube videos to prove the success of the operation. This comes about after the following statement by Anonymous: "Your support of the act is a signed death warrant to Sony Company and Associates. Therefore, yet again, we have decided to destroy your network. We will dismantle your phantom from the internet. Prepare to be extinguished. Justice will be swift, and it will be for the people, whether some like it or not,"

-Reference: <http://news.softpedia.com/news/Sony-Pictures-Website-and-Facebook-Page-Hacked-by-Anonymous-244839.shtml>

SCADA/ICS



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

**1. ICSA-12-006-01—3S SMART SOFTWARE SOLUTIONS CODESYS
VULNERABILITIES**

http://www.us-cert.gov/control_systems/pdf/ICSA-12-006-01.pdf

**2. ICSA-11-343-01—SIEMENS FACTORYLINK MULTIPLE ACTIVEX
VULNERABILITIES**

http://www.us-cert.gov/control_systems/pdf/ICSA-11-343-01.pdf

**3. ICSA-11-332-01A—INVENSYS WONDERWARE INBATCH ACTIVEX
VULNERABILITIES**

http://www.us-cert.gov/control_systems/pdf/ICSA-11-332-01A.pdf

**4. ICSA-11-362-01—SCADATEC SCADAPHONE/MODBUS TAGSERVER
BUFFER OVERFLOW**

http://www.us-cert.gov/control_systems/pdf/ICSA-11-362-01.pdf

5. ICSA-11-298-01A—SIELCO SYSTEMI WINLOG BUFFER OVERFLOW

http://www.us-cert.gov/control_systems/pdf/ICSA-11-298-01A.pdf

6. ICSB-11-327-01—ILLINOIS WATER PUMP FAILURE REPORT

http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf

**7. ICSA-11-361-01— SIEMENS AUTOMATION LICENSE MANAGER MULTIPLE
VULNERABILITIES**

http://www.us-cert.gov/control_systems/pdf/ICSA-11-361-01.pdf

8. ICSA-11-356-01 - Siemens SIMATIC HMI Authentication Vulnerabilities

http://www.us-cert.gov/control_systems/pdf/ICSA-11-356-01.pdf

9. ICSA-11-355-02 - WellinTech KingView Buffer Overflow

http://www.us-cert.gov/control_systems/pdf/ICSA-11-355-02.pdf

10. ICSA-11-355-01 - 7-Technologies IGSS Buffer Overflow Vulnerability

http://www.us-cert.gov/control_systems/pdf/ICSA-11-355-01.pdf



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

Noteworthy News

5. Canada Post is warning its customers that a circulating email that claims price discrepancies between corporate and private postal outlets is fake.

The email, purportedly from a customer, claims Canadians can ship the exact same packages out of corporate outlets for less. This is the second time the email has surfaced in more than a year, said Canada Post spokeswoman Anick Losier. The same email made the rounds last December. The corporation is also not sure whether the email is spam and where it originates from.

- Reference:

<http://www.canada.com/Canada+Post+warns+customers+about+fake+email/5883970/story.html>

6. Exploit Kits Now Updated With New Wares Before Patches Are Ready

The creators and maintainers of exploit kits often rely on public reports of new exploits and proof-of-concept exploit code in order to be able to add new exploits to their software. And in many cases, the exploits included in kits such as Black Hole and Eleonore and others will be for vulnerabilities that are older and have long since been patched. But, if recent events are any indication, that could be changing. In mid-October, details of a new Java vulnerability emerged in various places, and descriptions of the flaw showed it to be a serious one that could lead to remote code execution. The CVE-2011-3544 vulnerability, though serious, was just one of many that had been found in various Java components in recent months, and there already were plenty of others in the exploit kits that were being used in attacks.

- Reference: http://threatpost.com/en_us/blogs/exploit-kits-now-updated-new-wares-patches-are-ready-122011

7. Critical holes in Firefox, Thunderbird and SeaMonkey.

Mozilla developers not only gave the Firefox browser a faster JavaScript engine with their update to version 9.0, but they also closed various critical security holes. One critical flaw in previous versions of the browser allows an embedded OGG video element of “extreme” size to cause a crash that can potentially be exploited to inject malicious code. However, Mozilla is currently keeping the specific details of this confidentially disclosed vulnerability a secret. Mozilla closed a hole that allowed attackers to access out-of-bounds memory areas and inject malicious code via specially crafted SVG files. Another critical issue addressed in Firefox 9.0 is a currently unspecified and potentially exploitable crash in the YARR regular expression library. Mozilla also took the opportunity in 9.0 to close other critical memory bugs. The vulnerabilities also exist in previous versions of SeaMonkey and are addressed in the Seamonkey 2.6 update. The Thunderbird e-mail client is vulnerable, but only the first vulnerability mentioned is rated as critical. Version 9.0 of Thunderbird will fix the issues but has not yet been released.”



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

- Reference: <http://www.h-online.com/security/news/item/Critical-holes-in-Firefox-Thunderbird-and-SeaMonkey-1399340.html>

8. Anonymous aims to make US Senators accountable for their votes.

A group of Anonymous-affiliated hackers has made public a considerable amount of detailed personal information of the majority of the 86 US Senators that voted for the National Defense Authorization Act (NDAA). The Pastebin entry includes information such as dates of birth, spouse and children names, addresses, phone numbers, Twitter accounts, memberships in various committees, information about education, profession and religion, their staff, previous votes on a number of issues, their campaign contributors, suites filed against them, and more. The hackers don't claim to have stolen the information following a breach, and the document seems to have been compiled from information collected from a variety of sources accessible to the public.

- Reference: <http://www.net-security.org/secworld.php?id=12125>

9. Microsoft confirms Windows vulnerability "Microsoft has posted on its German language

Chief Security Advisor Blog about the Windows vulnerability reported last Tuesday. The post states that the company was able to reproduce a situation in which a specially crafted HTML page could cause a blue screen when opened with Safari on a 64-bit system. However, "at this time, our colleagues in the US do not believe that the vulnerability is capable of infecting Windows systems with malware", so the company will "most likely not publish a security advisory for this vulnerability" – but since the investigation has not yet been concluded, a final decision has yet to be reached. Microsoft has not been able to reproduce the bug on 32-bit systems, which corresponds to the observations of The H's associates at heise Security. According to the blog entry, Microsoft is working with Apple to find out more about the context which leads to the crash. The memory error occurs in the Windows system file, win32k.sys, which means that it could possibly also be created without Safari – and maybe even on 32-bit systems. Although the vulnerability lies not in the browser but in this Windows component, the relevant function is frequently called by browsers. Microsoft considers that, for this reason, Internet Explorer versions prior to 9 could be affected by this problem and recommends that individuals and business users should upgrade to the latest version. Security firm Secunia rated the vulnerability as "highly critical", since it could lead to the injection and execution of malicious code. There is as yet no exploit and the Microsoft posting states that the company considers any wide-ranging exploitation of this vulnerability to be unlikely.

- Reference: <http://www.h-online.com/security/news/item/Microsoft-confirms-Windows-vulnerability-1400353.html>

10. New Facebook clickjacking scam spreads like fire

It hooks them with links to titillating, disgusting or "amazing" videos that their friends apparently "liked", but once they click on the link, they are redirected to a splash page where they are asked to jump through some hoops in order to watch the video. Unfortunately, their clicks are hijacked to "like" the video without their knowledge and to post the same bait message on their own Walls, while they are redirected to a page seemingly containing that and other interesting videos. The



Public Safety
Canada

Sécurité publique
Canada

TLP: AMBER

Canada

scammers effect the clickjacking and redirection by using a number of JavaScripts, and land the user on one of around 300 similar pages that contain the video and a bucketful of link ads. "The JavaScript code is obfuscated and packed, this makes the entire debugging more difficult, but during the research I have identified several domains connected to this scam," says Kaspersky Lab Expert David Jacoby. "It also seems that they use redirectors to prevent URL/Domain blacklisting, and there are also several different scams on each server."

Reference: <http://www.net-security.org/secworld.php?id=12156>

11. Team Black Hat gave warning to Anonymous

They told that what Anonymous is doing is fully wrong and they dont scare of Anonymous. They said "Anonymous is a group of Script Kiddies"....They told that they are exploiting Anonymous IRC channel and they also caused the down time of their channels several weeks ago....They also mentioned about their Hactivist mission and also told that they are secretly observing every step of Anonymous. They added that the Hactivist mission is like physically attacking on religion. The Team Black Hat also mentioned about the Sony Network Hacking by Anonymous and they are very worried because of Anonymous had stolen millions of user accounts where most of them were children children aged between 10 and 16. Team Black Hat said that Anonymous fear them. And in the last sentence they told that Cyber War has started...

- Reference: <http://www.security-ray.com/2011/12/team-black-hat-gave-warning-to.html>

12. Anti-spam plan lacks teeth: prof

If you still find your e-mail inbox inundated daily with unwanted messages from far away royalty offering you free money or companies claiming they'll send you pharmaceuticals at a fraction of their price, you were likely pleased with the federal government's announcement of anti-spam legislation. But Dr. David Skillicorn, a professor at Queen's School of computing and computer security expert, doesn't think the federal government has the right plan in place for enforcing that legislation. His work with the laboratory has him investigating problems with cyber security, counter-terrorism, financial fraud and some law enforcement, Skillicorn explained. And from where he stands, the anti-spam centre the federal government is set to launch simply doesn't make sense. "I think the legislation is a good idea, but the idea of a spam reporting centre is completely unworkable, technically," Skillicorn explained.

- Reference: http://www.infomedia.gc.ca/ps-sp/articles/unrestricted/2012/01/ps-20121573845_12.htm

Breault, Stephen

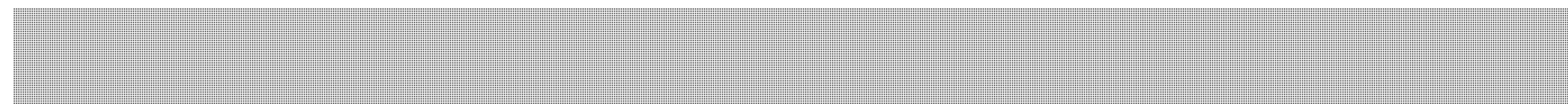
From: Champoux, Martin
Sent: Thursday, March 22, 2012 2:52 PM
To: Beaudoin, Luc
Subject: RE: AC 2971 cURL vulnerability disclosure

Merci

From: Beaudoin, Luc
Sent: Thursday, March 22, 2012 1:55 PM
To: Anderson, Windy
Cc: Champoux, Martin
Subject: AC 2971 cURL vulnerability disclosure

s.16(2)(c)
s.20(1)(c)

FYI



Vendors potentially affected were publicly identified on this recent (8 March) post which also indentified CCIRC.

Luc

Luc Beaudoin, P.Eng, MSc, MBA
Chief Cyber Operations | Chef des opérations cybernétiques Canadian Cyber Incident Response Centre | Centre
canadien de réponse aux incidents cybernétiques Public Safety Canada | Sécurité publique Canada Telephone |
Téléphone +1 613-991-9949 Facsimile | Télécopieur +1 613-991-3574 luc.beaudoin@ps-sp.gc.ca
<<mailto:luc.beaudoin@ps-sp.gc.ca>> PublicSafety.gc.ca Government of Canada | Gouvernement du Canada