Gmail

Samuel Huntley <samhuntley84@gmail.com>

Call With Comcast Security

32 messages

Carrera, Lyza <Lyza_Carrera@cable.comcast.com> Fri, Jun 10, 2016 at 8:36 PM
To: "samhuntley84@gmail.com" <samhuntley84@gmail.com>

Hi Sam,

I'm the Executive Assistant for the Comcast Cyber Security team. Jim Hoelsworth reached out to you yesterday to schedule a meeting today. We are available at 11:30am today to speak with you. The dial-in for the conference bridge is:

641-715-3580

Passcode: 620436#

Please respond to this email to confirm your availability at 11:30am today.

Thank you,

Lyza J Carrera / Executive Assistant to:

John Kelly - Vice President of Cybersecurity Threat Response & Engineering

650 Centerton Road Moorestown, NJ 08057 (p) 856-675-5101 (f) 856-638-4168

Lyza_Carrera@Cable.Comcast.com

COMCAST

Carrera, Lyza <Lyza_Carrera@cable.comcast.com> Fri, Jun 10, 2016 at 9:22 PM
To: "samhuntley84@gmail.com" <samhuntley84@gmail.com>

Hi Sam,

Since 11:30 was not a good time for you today, we'd like to offer Monday the 13th at 11am or 3pm as options for a 30 minute call with John and Jorge.

Please let me know if 11am or 3pm works so I can send you a calendar invite.

Thank you,

Lyza J Carrera / Executive Assistant to:

John Kelly - Vice President of Cybersecurity Threat Response & Engineering

650 Centerton Road Moorestown, NJ 08057 (p) 856-675-5101 (f) 856-638-4168

Lyza_Carrera@Cable.Comcast.com

COMCAST

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Fri, Jun 10, 2016 at 9:30 PM
To: "Carrera, Lyza" <Lyza_Carrera@cable.comcast.com>

Hi Careera,

Sorry I missed this email before as I am traveling.I am available now and 1 pm EST if you would like to talk. Otherwise it will have to be a couple of weeks down the line as I am traveling for next few weeks.

The other option is that you can send me any questions on email and I can respond to them. That would be the best option if we cannot do it today.

Thanks
Samuel Huntley
[Quoted text hidden]

--
Thanks,
Samuel Huntley

Carrera, Lyza <Lyza_Carrera@cable.comcast.com> Fri, Jun 10, 2016 at 9:56 PM
To: Samuel Huntley <samhuntley84@gmail.com>

Hi Sam,

We did not necessarily have questions for you since we met with Arris and they provided us all the information we needed. We want to discuss our remediation timelines so you are aware of those. If you become available within the next two weeks, reach out to us and we will meet with you. If not, let's get something on the calendar upon your return so that we can provide an update on where we are at that point.

We appreciate you reaching out to Arris to informed them of the two issues. We certainly take cybersecurity seriously so we have already our remediation efforts.

Let us know if there is anything else that you wanted to communicate to us or needed from us.

Lyza J Carrera

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Fri, Jun 10, 2016 at 10:05 PM
To: "Carrera, Lyza" <Lyza_Carrera@cable.comcast.com>
Cc: "Palmer, Douglas" <Douglas.Palmer@arris.com>, "Hoelsworth, James" <James_Hoelsworth@cable.comcast.com>

Hi Lyza,

Sure that sounds great.Also in that case if you don't mind sending me the approximate timeline that you guys have planned for remediating the issues, then that would be great.

That way I can plan to coordinate the public disclosure accordingly. Appreciate your response with this. Let me know if you need anything else.
[Quoted text hidden]
--
Thanks,
Samuel Huntley

Palmer, Douglas <Douglas.Palmer@arris.com> Sat, Jun 11, 2016 at 12:18 AM
To: Samuel Huntley <samhuntley84@gmail.com>

… thanks for the "fyi".

Doug

[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@cable.comcast.com> Sun, Jun 12, 2016 at 6:46 PM
To: Samuel Huntley <samhuntley84@gmail.com>

Hey Sam,
I was told your traveling for the next two weeks. Can we setup a call once you get back to discuss the vulnerabilities? We will be able to discuss remediation details at that time. Thanks again.

Sent from my iPhone
[Quoted text hidden]

> [Quoted text hidden]
> [Quoted text hidden]
>
> > [Quoted text hidden]
> >
> > Samuel Huntley

> [Quoted text hidden]
>
> > [Quoted text hidden]
> > [Quoted text hidden]
> >
> > <image001.png>
> >
> > ---
> >
> > **From:** Carrera, Lyza
> > **Sent:** Friday, June 10, 2016 11:07 AM
> > **To:** 'samhuntley84@gmail.com' <samhuntley84@gmail.com>
> > **Subject:** Call With Comcast Security
> >
> > Hi Sam,
> >
> > I'm the Executive Assistant for the Comcast Cyber Security team. Jim Hoelsworth reached out to you yesterday to schedule a meeting today. We are available at 11:30am today to speak with you. The dial-in for the conference bridge is:
> >
> > 641-715-3580
> >
> > Passcode: 620436#
> >
> > Please respond to this email to confirm your availability at 11:30am today.
> >
> > Thank you,
> >
> > Lyza J Carrera / Executive Assistant to:
> >
> > John Kelly - Vice President of Cybersecurity Threat Response & Engineering
> >
> > 650 Centerton Road Moorestown, NJ 08057   (p) 856-675-5101 (f) 856-638-4168
> >
> > Lyza_Carrera@Cable.Comcast.com
> >
> > <image001.png>
>
> --
>
> Thanks,

> Samuel Huntley

--
Thanks,
Samuel Huntley

image001.png
9K

Samuel Huntley <samhuntley84@gmail.com> Mon, Jun 13, 2016 at 4:48 AM
To: "Hoelsworth, James" <James_Hoelsworth@cable.comcast.com>

Hi James,

I am traveling outside USA starting tomorrow and will be gone for a few months. So unfortunately email will be the best way for any communication. Would you have an approximate estimate of when would the issues be fixed?

Also one more quick and gentle note, I did test this issue against a Business Comcast router (it was a Cisco make) and it seems to have the issue as well. I guess in that case I assume when you fix the issue for this router, it will be patched on other devices as well.

Thanks,
Samuel Huntley
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Mon, Jun 20, 2016 at 3:44 AM
To: "Hoelsworth, James" <James_Hoelsworth@cable.comcast.com>, "Carrera, Lyza" <Lyza_Carrera@cable.comcast.com>
Cc: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James/Lyza,

Any update on the remediation timeline for the security issues that were discovered? I would appreciate if you can let me know about it.

Thanks,
Samuel Huntley
[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@comcast.com> Tue, Jun 21, 2016 at 12:24 AM
To: Samuel Huntley <samhuntley84@gmail.com>, "Carrera, Lyza" <Lyza_Carrera@comcast.com>
Cc: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Samuel,

Thanks again for reporting this issue. Our developers are actively working on a patch now. If you can join a call, I would be happy to discuss more details with you. Let me know a date and time (EST) that works best for you, I can make any accommodation including later in the evening or weekend.

One other note, can you provide more details around the cisco CSRF you found? Ideally the make / model of the affected equipment would be helpful. I want to ensure that the patch we are working on will address this issue as well.

I look forward to speaking with you at your earliest convenience including upon your return from travel, if that works best.

Thanks.

James Hoelsworth
Sr. Manager, Security Fusion Center
National Security Operations
650 Centerton Rd | Moorestown, NJ 08057
O: 856-675-5192 | C: 856-912-4901 | SRC: 1-877-249-7306
James_Hoelsworth@cable.comcast.com

From: Samuel Huntley <samhuntley84@gmail.com>
Date: Sunday, June 19, 2016 at 6:14 PM
To: "Hoelsworth, James" <James_Hoelsworth@cable.comcast.com>, "Carrera, Lyza" <Lyza_Carrera@cable.comcast.com>
Cc: "Palmer, Douglas" <Douglas.Palmer@arris.com>

[Quoted text hidden]

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Wed, Jun 22, 2016 at 7:24 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

I guess since I am traveling abroad it might be harder to get together on a call especially with the time difference and all. It seems that you are all set with the issues itself, which is good in itself. Due to travel and time difference it might be harder to determine when we can get together on a call, lets keep some approximate estimate for the remediation timeline.

Usually I like to wait 150-180 days from the date of disclosing to the owner/vendor/3rd party personnel before disclosing the issue publicly. Kindly let me know if that sounds like a good time frame to you.

PS: Also a gentle note, unfortunately I don't have access to the Cisco device, so I might need to get that information to you a little later.

Thanks,
Samuel Huntley
[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@comcast.com> Sat, Jun 25, 2016 at 4:13 AM
To: Samuel Huntley <samhuntley84@gmail.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Sam,
Completely understand the logistics issues. The timeline you proposed should work for us. We will keep you posted if for any reason that changes.

If at all possible, please keep me posted on the model of the Cisco device. A couple of questions that might help me narrow this down a little, and ensure that our patche(s) will address the Cisco vulnerability.

- Did the web UI look the same as the Arris UI?
- Are you sure this was a business class device?
    - I completely understand if you do not wish to share any account info, but if you could provide a phone number or account number it would be a huge help.

The reason for these questions is that we have many different types of cisco modems on our network and some of these we manage the code for, others cisco managed their own code. So there is a chance we will be addressing the issue, or I may need to bring in Cisco, depending on these details.

Keep me posted and thanks for all your assistance.

Sent from my iPhone

On Jun 21, 2016, at 9:54 PM, Samuel Huntley <samhuntley84@gmail.com> wrote:

> Hi James,
>
> I guess since I am traveling abroad it might be harder to get together on a call especially with the time difference and all. It seems that you are all set with the issues itself, which is good in itself. Due to travel and time difference it might be harder to determine when we can get together on a call, lets keep some approximate estimate for the remediation timeline.
>
> Usually I like to wait 150-180 days from the date of disclosing to the owner/vendor/3rd party personnel before disclosing the issue publicly. Kindly let me know if that sounds like a good time frame to you.
>
> PS: Also a gentle note, unfortunately I don't have access to the Cisco device, so I might need to get that information to you a little later.
>
> Thanks,
> Samuel Huntley
>
> On Mon, Jun 20, 2016 at 2:54 PM, Hoelsworth, James <James_Hoelsworth@comcast.com> wrote:
>
>> Samuel,
>>
>> Thanks again for reporting this issue. Our developers are actively working on a patch now. If you can join a call, I would be happy to discuss more details with you. Let me know a date and time (EST) that works best for you, I can make any accommodation including later in the evening or weekend.
>>
>> One other note, can you provide more details around the cisco CSRF you found? Ideally the make / model of the affected equipment would be helpful. I want to ensure that the patch we are working on will address this issue as well.
>>
>> I look forward to speaking with you at your earliest convenience including upon your return from travel, if that works best.
>>
>> Thanks.

> James Hoelsworth
> Sr. Manager, Security Fusion Center
> National Security Operations
> 650 Centerton Rd | Moorestown, NJ 08057
> O: 856-675-5192 | C: 856-912-4901 | SRC: 1-877-249-7306
> James_Hoelsworth@cable.comcast.com
>
> <image001.png>
>
> [Quoted text hidden]

COMCAST **image001.png**
4K

Samuel Huntley <samhuntley84@gmail.com> Mon, Jun 27, 2016 at 7:00 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

Sounds good. I will have to check to get you the details of Cisco model. But it's WebUI was exactly the same as the Arris model as far as I recollect and yes it is a business class device as it is used under a Comcast Business account.

Thanks,
Samuel Huntley
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Sat, Jul 9, 2016 at 3:40 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

Here are the details of the Cisco router that had the same issue at least from preliminary testing that I had did almost 1 month ago:

Model: DPC3941B
Hardware Revision: 1.0

Thanks,
Samuel Huntley
[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@comcast.com> Sat, Jul 9, 2016 at 3:50 AM
To: Samuel Huntley <samhuntley84@gmail.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Thanks Sam,
I forwarded this to my developers. Thanks for the info. Will keep you posted.

Sent from my iPhone
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Mon, Sep 12, 2016 at 7:28 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

Just wanted to check in and see how things were progressing?

Thanks,
Samuel Huntley
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Mon, Oct 3, 2016 at 1:46 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

I have not heard anything back from you, so wanted to ensure that we are still on target to get the security issue fixed in next 1 month right? As I plan to release the details by end of November, this year. Let me know about it.

Thanks,
Samuel Huntley
[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@comcast.com> Mon, Oct 3, 2016 at 2:04 AM
To: Samuel Huntley <samhuntley84@gmail.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hey Samuel,
Yes sorry, I missed your previous email. I know the team is testing the patches in qa. I believe we will be ready by end of November to meet your timeline for disclosure. Thanks for checking in. If you don't mind, let's circle back at the end Oct? Does that work for you?

Sent from my iPhone
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Fri, Dec 23, 2016 at 3:46 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

I just wanted to check in and make sure that the vulnerability was taken care of at this point, as I plan to release the vulnerability details out next week.

Thanks,
Samuel Huntley
[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@comcast.com> Sat, Dec 24, 2016 at 6:21 AM
To: Samuel Huntley <samhuntley84@gmail.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Sam,
Thanks for reaching out. We released a patch that remediates the issue you identified relating to Arris devices on our network. This went live to all affected devices on our network in late Oct, early Nov.

However, during our research we identified a related issue with Cisco devices. Our initial patch is not working as expected for the Cisco platform. We have developed a new patch just for the Cisco platform and it is currently going through testing. We expect a full deployment by January 31.

Is there anyway you could push your release until this patch goes live? We would prefer to have the issue fully addressed across all the platform before the announcement. I really appreciate your assistance. Thank you again for all your hard work.

Sent from my iPhone
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Sun, Dec 25, 2016 at 7:51 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

Hmm, okay I can wait a few more days I suppose. Just so I understand, is this the same issue with Cisco devices that I had mentioned or is this a separate one?

Thanks,
Samuel Huntley
[Quoted text hidden]

Hoelsworth, James <James_Hoelsworth@comcast.com> Tue, Dec 27, 2016 at 5:43 AM
To: Samuel Huntley <samhuntley84@gmail.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hey Sam,
The patch will fix the issue you identified with the Cisco platform. The original patch we rolled out for Arris and Cisco did not work as expected on the Cisco platform so the team developed a new fix. The arris patch was deployed and is working as expected. Thank you for your patience and understanding.

Sent from my iPhone
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Wed, Dec 28, 2016 at 7:21 AM
To: "Hoelsworth, James" <James_Hoelsworth@comcast.com>
Cc: "Carrera, Lyza" <Lyza_Carrera@comcast.com>, "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi James,

Okay I will wait till the end of January, 2017 to release the details.

Thanks,
Samuel Huntley
[Quoted text hidden]

Davis, Noopur <Noopur_Davis@comcast.com> Sat, Jan 21, 2017 at 1:16 AM
To: "samhuntley84@gmail.com" <samhuntley84@gmail.com>
Cc: "Hoelsworth, James" <James_Hoelsworth@comcast.com>

Dear Sam

I’m following up on the issue you’ve been discussing with a member of my team, James Hoelsworth. My name is Noopur Davis, I’m the Chief Product and Information Security Officer for Comcast Cable, and I wanted to introduce myself, thank you for your important work on this issue, and share an update on the current status.

We are on track to remediate the issue you identified on both Cisco and ARRIS devices running our RDK-B firmware by the end of January 2017. However, as part of our ongoing research, we also identified a smaller number of devices running older legacy firmware, which are subject to the same issue you identified. We are transitioning those devices to the newer, remediated RDK-B firmware, but unfortunately that process will not be completed until the end of March 2017.

We appreciate your working with us and your patience to date. We will let you know once we are fully remediated across all platforms and firmware and ask that you publish your report at that time.

Please let me know if you have any questions about this. In any case, thank you again for your work on this issue. Researchers like you do work of critical importance, and we value your work highly.

Best,

Noopur

-

Noopur Davis

SVP Comcast Technology + Product

Chief Product and Information Security Officer, Comcast Cable

Cell: 215-581-7122

Office: 215-286-8879

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Sat, Jan 21, 2017 at 5:15 AM
To: "Davis, Noopur" <Noopur_Davis@comcast.com>
Cc: "Hoelsworth, James" <James_Hoelsworth@comcast.com>

Hi Noopur,

Nice to meet you virtually. I appreciate you letting me know the status and progress on the firmware fixes. However it has been almost more than 8 months that the team has been working on fixing the issue. I understand that product life cycles are complicated and need some time especially from bug fixing perspective. As I understand the importance of the issue and its possible impact on Comcast customers,

I will wait on releasing any specific details and the POC code for the vulnerability for now, but will just mention the announcement that security issue has been identified in Comcast devices and the team is working on fixing it. Once you have the issues re-mediated around March time frame, then I can release the specific details of the router vulnerable as well as the security issue details.

Again, I hope you understand my intention in this case is not to cause any reputation damage for Comcast, but just protect the victims that might be susceptible to the issue. Kindly let me know if you need any thing else.

Thanks,
Samuel Huntley
[Quoted text hidden]

Davis, Noopur <Noopur_Davis@comcast.com> Sat, Jan 21, 2017 at 5:35 AM
To: Samuel Huntley <samhuntley84@gmail.com>
Cc: "Hoelsworth, James" <James_Hoelsworth@comcast.com>

Sam

Thanks for your quick response. Let me get with my team next week and then get back to you.

Best,
Noopur

Sent from my iPhone
[Quoted text hidden]

Davis, Noopur <Noopur_Davis@comcast.com> Mon, Jan 23, 2017 at 6:57 PM
To: Samuel Huntley <samhuntley84@gmail.com>

Hi Sam:

Following-up from Friday: we ask that you give us until the end of this month, as previously you agreed to, before disclosing any information.

We will circle back with you by the end of this month with the latest status.

Best,

Noopur

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Tue, Jan 24, 2017 at 7:33 AM
To: "Davis, Noopur" <Noopur_Davis@comcast.com>

Hi Noopur,

Sure that should be fine. At the end of the month, I will share with you guys the announcement that I will be making before providing it out there.

Thanks,
Samuel Huntley
[Quoted text hidden]

Davis, Noopur <Noopur_Davis@comcast.com> Tue, Jan 24, 2017 at 7:36 AM
To: Samuel Huntley <samhuntley84@gmail.com>

Thank you, Sam.

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Sun, Feb 12, 2017 at 6:10 AM
To: "Davis, Noopur" <Noopur_Davis@comcast.com>

Hi Noopur,

I am planning to share some of the details next week about the Cisco and Arris Modem based command injection vulnerability.I will hold on sharing the actual POC till March as discussed before.

Thanks,
Samuel Huntley
[Quoted text hidden]

Davis, Noopur <Noopur_Davis@comcast.com> Sun, Feb 12, 2017 at 6:32 AM
To: Samuel Huntley <samhuntley84@gmail.com>

Thank you for letting me know. We are actually ahead of schedule in getting this remediated on the last of our native devices, and have been rolling out the fix this last week. Hoping to get the last remaining devices remediated over the next few weeks.

Can you share the actual wording you will be using?

Best,
Noopur

Sent from my iPhone
[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com> Mon, Feb 13, 2017 at 2:14 AM
To: "Davis, Noopur" <Noopur_Davis@comcast.com>

Hi Noopur,

Sure I will do that as soon as I have it ready.

Thanks,
Samuel Huntley
[Quoted text hidden]