Security Issue

13 messages

Palmer, Douglas <Douglas.Palmer@arris.com> Mon, Jun 6, 2016 at 8:13 PM
To: "samhuntley84@gmail.com" <samhuntley84@gmail.com>

Hi Sam,

I'm Doug Palmer, the global quality director for ARRIS home products including modems.

Thanks for reaching out about a potential security issue with one of our modems. As you can imagine, we are always looking to make our product hardware and software robust to security vulnerabilities, so I'm very interested to hear what you have found.

Would you have a few minutes sometime in the next week for a brief discussion?

Best,

Doug

Doug Palmer

Business Quality Director

ARRIS

o: +1 215.323.2308

c: +1 215.778.2492

e: Douglas.Palmer@arris.com

w: www.arris.com

Samuel Huntley <samhuntley84@gmail.com> Tue, Jun 7, 2016 at 4:53 AM
To: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Doug,

        Sure, I can send you the details on the email if you would like or if you like to talk, then we can do the discussion sometime later this week and I can call you at your office or cell number. Kindly let me know about it.

Thanks,
Samuel Huntley
[Quoted text hidden]

Palmer, Douglas <Douglas.Palmer@arris.com>   Tue, Jun 7, 2016 at 6:59 AM
To: Samuel Huntley <samhuntley84@gmail.com>

Sam,

A call may work better if we have a lot of questions. I may also want to bring in my security expert depending on what the issue is. So my preference would be, is this is agreeable to you, to ask you to send a summary email out in advance of a call later this week, and to let me know what are some good times based on your schedule.

Thanks again for alerting ARRIS of a security concern.

Doug

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com>   Tue, Jun 7, 2016 at 7:35 AM
To: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Doug,

        Sure the issue is command injection that exists in Arris TG1682G modem. This can be exploited by combining the fact that there is no cross-site request forgery protection on any web request. Attached is the web request file, an image file showing the software version, a video showing the actual command injection working and also a proof of concept cross site request forgery html file.

Kindly let me know if you need anything else. Also please let me know after reviewing when you plan to fix the issue as well as the possible time frame so I can plan to release the details accordingly.

Thanks,
Samuel Huntley
[Quoted text hidden]

📄 **Arris Modem Command Injection.zip**
10208K

Palmer, Douglas <Douglas.Palmer@arris.com>   Tue, Jun 7, 2016 at 5:24 PM
To: Samuel Huntley <samhuntley84@gmail.com>

Sam,

Thanks for the detail. Looks like it's a Rev. 9.0 TG1682G running on a Comcast network.

Can you also send the software version?

Let's meet on Thu/Fri for a few minutes and I'll have some answers by then.

Regards,

[Quoted text hidden]

Palmer, Douglas <Douglas.Palmer@arris.com>   Tue, Jun 7, 2016 at 5:33 PM
To: Samuel Huntley <samhuntley84@gmail.com>

nm – I see the SW version in the zip package - thanks

From: Palmer, Douglas
Sent: Tuesday, June 07, 2016 7:55 AM
To: 'Samuel Huntley' <samhuntley84@gmail.com>
Subject: RE: Security Issue

Sam,

Thanks for the detail. Looks like it's a Rev. 9.0 TG1682G running on a Comcast network.

Can you also send the software version?

Let's meet on Thu/Fri for a few minutes and I'll have some answers by then.

Regards,

Doug

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com>   Tue, Jun 7, 2016 at 9:08 PM
To: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Doug,

    Thanks that should work just fine.

Thanks,
Samuel Huntley
[Quoted text hidden]

--
Thanks,
Samuel Huntley

Samuel Huntley <samhuntley84@gmail.com>   Thu, Jun 9, 2016 at 6:26 AM
To: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Doug,

      Would tomorrow work for you so we can discuss if you like as Friday I am out for some personal work? Let me know about it.

Thanks,
Samuel Huntley
[Quoted text hidden]

Palmer, Douglas <Douglas.Palmer@arris.com>   Thu, Jun 9, 2016 at 8:01 AM
To: Samuel Huntley <samhuntley84@gmail.com>

Hi Sam,

Afternoon or evening is good. What's a good time for you?

Doug

Samuel Huntley <samhuntley84@gmail.com> wrote:

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com>   Thu, Jun 9, 2016 at 9:13 AM
To: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Doug,

      Sure tomorrow afternoon around 3 pm EST works for me.Let me know if that works for you and a good number to reach you and I can call then.

Thanks
Samuel Huntley
[Quoted text hidden]

--
Thanks,
Samuel Huntley

Palmer, Douglas <Douglas.Palmer@arris.com>   Thu, Jun 9, 2016 at 3:29 PM
To: Samuel Huntley <samhuntley84@gmail.com>

3p is good. Please call me st 215.323.2308

Doug

Samuel Huntley <samhuntley84@gmail.com> wrote:

[Quoted text hidden]

Samuel Huntley <samhuntley84@gmail.com>   Fri, Jun 10, 2016 at 1:22 AM
To: "Palmer, Douglas" <Douglas.Palmer@arris.com>

Hi Doug,

Thanks appreciate the call today.As per our discussion since the vulnerable code belongs to comcast, it seems that they are already aware of this issue and are working on it. If they don't contact me by next week Wednesday, I will contact you again.

Thanks for coordinating this.

Thanks
Samuel Huntley
[Quoted text hidden]

--
Thanks,
Samuel Huntley

Palmer, Douglas <Douglas.Palmer@arris.com>   Fri, Jun 10, 2016 at 1:50 AM
To: Samuel Huntley <samhuntley84@gmail.com>

Thanks Sam.

Samuel Huntley <samhuntley84@gmail.com> wrote:

[Quoted text hidden]