From: White, Douglas A. / UDEL
Date: February 28, 2014 1:49:37 PM MST

Just a heads up that there are a few router vulnerabilities popping up in the security news lately.

Of note this week are Linksys and Asus models.

Throwing this out on the list as I can imagine that there are a few of us that're using these as buffers to the internet in our shops or on our RVs.

Make sure you've disabled the external management features of the routers as some of them were shipped with this feature enabled. That seems to be what's affecting the Linksys line.

Lots of more detailed info via the Security Now podcast show notes:

https://www.grc.com/sn/sn-443-notes.pdf

Doug

From: Thomas Wilson / CUNY Stonybrook
Date: March 1, 2014 10:16:17 AM MST

Hi Doug,

I like having external management enabled, it can be useful for remote troubleshooting. I'm not an expert on the complexities, so I have a few questions:

1) Does this vulnerability exist if remote management is turned on, even if the password is changed from the default?

2) "You can't hack what you can't see". Most of the time these routers default to "invisible", i.e. they don't respond to pings etc. Would a hacker just hit every IP address with the exploit and hope to get lucky?

3) How about updating the router firmware to DD-WRT, does that fix the problem?

http://www.dd-wrt.com/site/index

I do this to many of my routers - it very often gives a $60 home router the capabilities of a $200 plus enterprise router (WiFi repeater, Wifi as WAN, etc.).

Thanks for passing this along,
Tom

From: Toby Martin / OSU
Date: March 5, 2014 12:52:03 PM MST

Date: Sat, 1 Mar 2014 17:16:17 +0000
From: Thomas Wilson <thomas.wilson@stonybrook.edu>

I like having external management enabled, it can be useful for remote
troubleshooting. I'm not an expert on the complexities, so I have a few
questions:

Hi Tom,

Great questions! Of course the answers depend on the specific issues being addressed. Looking at the vunerabilities reffered to in <https://www.grc.com/sn/sn-443-notes.pdf> ...

1) Does this vulnerability exist if remote management is turned on, even if
the password is changed from the default?

Yes.

Asus:

"Default setting for the ftp-server was to allow anonymous login."

Linksys:

"Customers who have enabled the Remote Management Access

feature
can prevent further vulnerability to their network, by disabling the Remote Management Access feature and rebooting their router to remove the installed malware."

2) "You can't hack what you can't see". Most of the time these routers default to "invisible", i.e. they don't respond to pings etc. Would a hacker just hit every IP address with the exploit and hope to get lucky?

Yes. Most hackers just run a script that cycles through IP addresses.

3) How about updating the router firmware to DD-WRT, does that fix the
problem?

Yes. At least it fixes THIS problem :-)
Additionally, if you use a currently supported program, it gives you access
to security updates, rather than waiting for Asus or Linksys to release a
fix more than a year after the exploit has been announced.

- Toby

From: White, Douglas A / UDEL
Date: March 6, 2014 8:27:42 AM MST

Also, something to note on the Linksys router side is that Linksys was previously purchased by Cisco, who has now sold the Linksys line of consumer routers to Belkin. So now Belkin is the parent company of Linksys. Not sure what that means for the maintenance and upkeep for older Linksys-branded routers.

I've heard good things about the DD-WRT and Tomato open source replacements for the Linksys router stock firmware, but I haven't used them personally.

Doug