RISK ASSESSMENT / SECURITY & HACKTIVISM

Got an Asus router? Someone on your network can probably hack it

Root command execution bug invades most wireless routers.

by **Dan Goodin** - Jan 8, 2015 10:16am PST

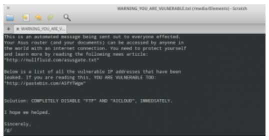
91

If you're running an Asus wireless router, chances are good that someone inside your network can take full administrative control of it thanks to a currently unpatched vulnerability in virtually all versions of the firmware, a security researcher said.

While the vulnerability isn't as serious as those that allow hackers on the Internet at large to compromise the devices, it's nonetheless concerning. People with administrative control can reroute everyone connected to malicious websites and possibly install alternate or even malicious firmware updates.

"I trust people that join my network to some degree, but I don't want them to be able to reconfigure the router," Joshua Drake, research director at Accuvant and the person who brought the vulnerability to light Thursday, told Ars. "I can't prevent them without this getting fixed (short of the workaround)."

FURTHER READING


WARNING_YOU_ARE_VULNERABLE.txt (/media/Elements) - Scratch

WARNING_YOU_ARE_V...

```
This is an automated message being sent out to everyone effected.
Your Asus router (and your documents) can be accessed by anyone in
the world with an internet connection. You need to protect yourself
and learn more by reading the following news article:
"http://nullfluid.com/asusgate.txt"

Below is a list of all the vulnerable IP addresses that have been
leaked. If you are reading this, YOU ARE VULNERABLE TOO:
"http://pastebin.com/ASfYTWgw"


Solution: COMPLETELY DISABLE "FTP" AND "AICLOUD", IMMEDIATELY.

I hope we helped.

Sincerely,
/g/
```

DEAR ASUS ROUTER USER: YOU'VE BEEN PWNED, THANKS TO EASILY EXPLOITED FLAW

Hackers expose eight-month-old Asus weakness by leaving note on victims' drives.

The vulnerability stems from a poorly coded service known as infosvr, which monitors the local area network for other connected routers. Infosvr runs with unfettered root privileges and contains an unauthenticated command execution bug. The result: anyone connected to the local network can gain control by sending a single user datagram protocol packet to the router. Drake said virtually all Asus wireless routers are susceptible. He said testing showed firmware version 3.0.0.376.2524-g0013f52 was vulnerable, but he assumes all other versions are also affected. The bug has been designated CVE-2014-~~10000~~9583.

Unless Asus releases a patch, there's little non-technical users can do to close the hole. More technically inclined people can use the vulnerability itself to turn off infosvr after each reboot. They can use the following command to do so.

```
$ ./asus-cmd "killall -9 infosvr"
[...]
```

Over the past 18 months, wireless routers from a variety of manufacturers have emerged as a popular target of in-the-wild hacks. Again, this latest vulnerability affecting Asus users is less serious since it doesn't permit hackers halfway around the world to gain entry. But it still could pose major problems for some people, particularly those who use Asus routers to run hotspots or other public Wi-Fi networks.

FURTHER READING

BIZARRE ATTACK INFECTS LINKSYS ROUTERS WITH SELF-REPLICATING MALWARE

Some 1,000 devices have been hit by the worm, which seeks out others to infect.

PROMOTED COMMENTS

BadSuperblock | Ars Scholae Palatinae jump to post

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Review: Mint 17.3 may be the best Linux desktop distro yet

If you don't want to think too hard about which OS you're using, Mint is for you.

WATCH ARS VIDEO

Ars visits Nest Labs

We learn about their programmable, self-learning, sensor-driven, Wi-Fi-enabled thermostats.

STAY IN THE KNOW WITH

LATEST NEWS

THAT ESCALATED QUICKLY

Martin Shkreli's other pharma company is dramatically collapsing

ROUNDTRIP TICKET TO THE IRON AGE

Scientists find 1500-year-old Viking settlement beneath new airport site

MINDLESS MUNCHING

Making healthy foods the default menu dupes people into eating better

Asian-American band "The

> JohnnyTheGeek wrote:
> If you trust someone to be on your network as a full access user. Why then is this such a big deal. Many devices on a network default to sharing and linking at least minimally together anyway. Much of the Asus line of routers are consumer driven anyway. I would be surprised if any sensitive business is using these types of routers. But even so, most should know who is using their local network and have a password on it. I guess its worthy note for a article but I doubt many will be so concerned about it.

I call this type of post the "I live alone" post.

I have secured my wireless network as much as I reasonably can from outsiders. But one time I let a friend from out of town stay with me with his wife and three kids. Within 5 seconds of coming in the door, the first thing the kids wanted to do was get their devices back onto the Internet, and naturally I couldn't say "You can't use my wifi." One of them is a technically savvy teenager. Sometimes it's difficult to deny certain people access to my LAN like that teenager, or like my brother, who I know could totally mess with certain wide-open (no password even possible for like my AV receiver) IP-accessible devices on my LAN if they wanted to. Those devices might not be mission critical, but the one that is, is my router, and I would not want some of these not-100%-trustworthy users to get into it via this vulnerability. (I know you can get around some of this if your router has a separate guest network.)

And of course your post doesn't address the "public hotspot" use case mentioned in the article at all...

1149 posts | registered Oct 17, 2008

READER COMMENTS 91

- - - -

Dan Goodin / Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

@dangoodin001 on Twitter

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE

Slants" overturns USPTO rule on "disparaging" trademarks

FOIA REINFORCEMENTS

Suspecting climate change conspiracy, Judicial Watch sues NOAA for scientists' e-mails

Progress! New CMOS chip can process both light and electricity

SITE LINKS MORE READING CONDE NAST SITES

About Us
Advertise with us
Contact Us
Reprints

SUBSCRIPTIONS

Subscribe to Ars

RSS Feeds
Newsletters

Visit Ars Technica UK

Reddit
Wired
Vanity Fair
Style
Details

Visit our sister sites

Subscribe to a magazine

VIEW MOBILE SITE

CONDÉ NAST