Millions of Home Routers at Risk?

- July 29, 2010
- By Sean Michael Kerner
-
- Submit Feedback »
- More by Author »

LAS VEGAS -- According to new research delivered today here at the Black Hat security conference, millions of home routers may have a serious security flaw.

In his presentation at Black Hat, security researcher Craig Heffner detailed how an external attacker could gain full control of a user's router and use that to gain access to the internal local area network (LAN). Though the implications are ominous, Heffner, also detailed a variety of steps users can take to protect themselves.

"The question is not how to hack the routers, that's easy," Heffner said. "The question is how to get access when you're not on the local LAN."

Every network router has both an external WAN interface, as well as an internal LAN interface. The WAN interface has the public IP address while the LAN interface is a private IP address. The way things are supposed to work is that external users are not supposed to be able to publicly access the router internals.

- Email Article
- Print Article
- Comment on this article

But Heffner said he was able to leverage DNS rebinding, which exposes the local private IP address and binds it to the public address. Heffner wrote a tool called Rebind to make it easier to automatically perform the whole operation. The Rebind tool is set to be freely available on the Google Code project hosting site.

The Rebind tool will serve up JavaScript code that enables the whole attack to occur. As such, a user would need to actually click on a link in order to execute the exploit. Once the user clicks on the malicious link, the Rebind tool gives the attacker the user's private IP address on the LAN.

"The attacker then gets access to the router and can browse the local LAN of the target user as if they were a user on the local LAN," Heffner said.

In an on-stage demo, Heffner showed how he could access an Actiontec router that is used by Verizon for its broadband customers.

Related Articles

- SSL Study Shows Most Sites Incorrectly Configured
- Cisco Details Enterprise Security Threats
- Popular Home Router Flaw Found
- Black Hat USA 2010 Preview
- Improve Your Wireless Security With the Right Routers

"Once I'm into your router I can put whatever tools I want and run them against your network," Heffner said. "The great thing about routers is that they're connected to the Internet and your LAN."

In addition to leveraging Rebind to access the LAN, Heffner noted it could potentially be used to turn the router into a proxy for other attacks.

Protecting your router

Like other speakers at Black Hat, Heffner didn't detail the security flaw to aid potential attackers, but rather to alert users and the relevant vendors.

Heffner suggested one preventative measure users can take is to change their firewall rules to

prevent an external IP from rebinding with internal ones. Additionally he suggested that it's likely a best practice for home users to just disable the http admin interface of their routers, if that's an option.

Another key thing that Heffner suggested users should do is change the default password for their home routers and to make sure that the router's firmware is up-to-date.

Heffner also called on router vendors to build in DNS Rebinding mitigations into their routers directly.

"The only router software that I know of that does this now is pfsense 2.0," Heffner said. "They contacted me when my Black Hat talk abstract went up."

Sean Michael Kerner is a senior editor at InternetNews.com , the news service of Internet.com , the network for technology professionals.

-webadmin- I have not validated any of this information yet but found it interesting nontheless. This is just another comfort level if you plan to use PFSense for SOHO deployment and research into this DNS exploit is certainly worth investigation to validate this articles content for correctness and accuracy. *Rebind PDF*

Update: 5-17-2011 TestedRouters *Routers that have been tested against this attack.* Updated Aug 3, 2010 by heffne...@gmail.com

Link Here...

Known Affected Routers

- ActionTec MI-424WR
- ActionTec GT704-WG
- ActionTec GT701-WG
- Asus WL-520gU
- Belkin F5D7230-4 v.2000
- ClearAccess AG-10

- D-Link DIR-300
- D-Link DIR-320
- DD-WRT
- Dell TrueMobile 2300
- Linksys BEFSR41
- Linksys BEFW11S4
- Linksys WRT-160N
- Linksys WRT54G3G-ST
- Linksys WRT54G v.3
- Linksys WRT54GL
- OpenWRT
- PFSense v1.2.3
- Thomson ST585v6

Known Unaffected Routers

- Belkin F5D7230-4 6.000
- Belkin F5D6231-4
- D-Link DI-524
- D-Link DI-624
- D-Link DIR-628
- D-Link DIR-655
- D-Link WBR-1310
- Linksys WRT54G2
- Linksys WRT54Gv5
- Netgear WGR614
- Netgear WNR834B