If your router is on this list, upgrade immediately!

Routers are vital components of network infrastructure that can last for decades. But if they get too old, hackers can exploit them to do bad things.

Routers are vital components of network infrastructure that can last for decades. But if they get too old, hackers can exploit them to do bad things.

Old Routers Are a Threat to Your Network

The FBI has uncovered a group of hackers exploiting old routers to carry out cyberattacks. The agency's announcement includes a list of 13 routers that have reached 'end of life' status, meaning they no longer receive software updates to fix known vulnerabilities.

The following routers are being targeted:

1. Cisco M10
2. Cisco Linksys E1500
3. Cisco Linksys E1550
4. Cisco Linksys WRT610N
5. Cisco Linksys E1000
6. Cradlepoint E100
7. Cradlepoint E300
8. Linksys E1200
9. Linksys E2500
10. Linksys E3200
11. Linksys WRT320N
12. Linksys E4200
13. Linksys WRT310N

All routers have a management interface that can be accessed by connecting to the router via Ethernet, Wi-Fi, or over the Internet. If the interface is exposed to the Internet, hackers can exploit known router vulnerabilities to upload malware and gain admin access.

The malware used in the attack, called TheMoon, was first discovered on compromised routers in 2014. The FBI alert states that it does not require a password to infect routers. The malware scans for open ports and sends commands to a vulnerable script on the router. Once the command is executed, it sets up a Command and Control Server (C2), which then responds with further instructions.

Malware uploaded to targeted routers allows hackers to maintain persistent access to the devices, allowing them to use them as part of larger botnets. The botnets are then used to launch coordinated DDoS attacks or sold as proxy services that hackers use to mask their IP addresses and identities.

The agency also seized two websites — Anyproxy and 5Socks — that were using hacked routers to provide proxy services to 'help cybercriminals hide their activities.' The websites have been updated to display the US Department of Justice's seizure notice.

How can users protect themselves?

If you are using one of the routers mentioned above, the best solution is to upgrade your router to a newer model. In addition to better security, you will also enjoy faster internet speeds and a more stable Wi-Fi connection. Even if your router is not on the list above but has reached the end of its life, replacing it is the right solution.

If you can't replace your router right away, disable any remote management or administration features in your router's control panel. The specific instructions for doing this will vary from router to router, so look up your router's model number for more information. Your router is one of the most vulnerable devices in your home and should be properly secured.

For those with newer routers, regularly check for updates to ensure your router is protected from any vulnerabilities that hackers may exploit. Unless you really need the remote management feature of your router, it's best to disable it for added protection.