Issued 4/25/17

25 Linksys Smart Wi-Fi Models Vulnerable to Attacks

Twenty-five Linksys router models are vulnerable to serious attacks that could have a huge security impact on owners. According to IOActive, these models are vulnerable to attacks that allow third parties to reboot, lock out and extract sensitive router data from affected devices.

The issue affects the latest Linksys Smart Wi-Fi Router brands, they say, identifying models using the latest 802.11N and 802.11AC standards as being at risk. IOActive researcher Tao Sauvage says they found ten vulnerabilities that impact the Linksys routers. During the investigation, 7,000 vulnerable routers were discovered to be in use. However, more than 100,000 additional routers vulnerable to the flaws could also be in use, which makes the situation a lot more problematic. "We found about 7,000 vulnerable devices exposed at the time of the search. It should be noted that this number does not take into account vulnerable devices protected by strict firewall rules or running behind another network appliance, which could still be compromised by attackers who have access to the individual or company's internal network," Sauvage notes.

Most of the vulnerable devices they discovered are in the United States (69%), while the rest are spread across the world, including in Canada, Hong Kong, Chile, the Netherlands, Venezuela, Argentina, Russia, Sweden, Norway, China, India, UK, Australia, and others. Linksys was informed about the vulnerabilities back on January 17 and has worked

alongside IOActive to check the customer advisory and the list of vulnerable routers. In fact, Linksys has released a security advisory which their advice every Linksys Smart Wi-Fi owner to read.

Users are also advised to change the default password of the Admin account to protect the web admin interface. A firmware update is in the works, but it may take a little bit more time before it is available. Until then, it's best for users to be cautious, enable automatic updates and disable the WiFi Guest Network if not in use, on top of changing the password. Here's the list of affected models:

- EA2700
- EA2750
- EA3500
- EA4500v3 - EA6100

- EA6200
- EA6300
- EA6350v2 - EA6350v3

- EA6400 - EA6500 - EA6700 - EA6900 - EA7300 - EA7400 - EA7500 - EA8300 - EA8500

- EA9200
- EA9400
- EA9500
- WRT1200AC
- WRT1900AC
- WRT1900ACS - WRT3200ACM