Fixes in the works for Moon-struck Linksys routers

February 18 2014, by Nancy Owano

(Phys.org) —Self-replicating malware has struck some older Linksys routers and Linksys has acknowledged awareness of the malware, called "TheMoon." They plan to make firmware fixes for all affected products available "Linksys will be working on the affected products with a firmware fix that is planned to be posted on our website in the coming weeks," according to a company statement. Only those routers with Remote Management Access enabled within the administrative settings are vulnerable. *Ars Technica* characterized the attack as one that infects home and small-office wireless routers from Linksys with self-replicating malware, likely by exploiting a code-execution vulnerability in the firmware.

As self-replicating malware, TheMoon takes advantage of the remote access feature. The attacker can grab access to the admin panel.

"Linksys ships these products with the Remote Management Access feature turned off by default," noted the company statement, which also said that the attack involves older E and N routers.

The official statement read: "Linksys is aware of the malware called "The Moon" that has affected select older Linksys E-Series routers and select older Wireless-N access points and routers."

The statement noted that the "exploit to bypass the admin authentication used by the worm only works when the Remote Management Access feature is enabled. Linksys ships these products with the Remote Management Access feature turned off by default. Customers who have not enabled the Remote Management Access feature are not susceptible to this specific malware. 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. Linksys will be working on the affected products with a firmware fix that is planned to be posted on our website in the coming weeks."

Linksys also has a page up that explains, step by step, how to avoid getting TheMoon malware, and describes how it behaves: "The Moon malware bypasses authentication on the router by logging in without actually knowing the admin credentials. Once infected, the router starts flooding the network with ports 80 and 8080 outbound traffic, resulting in heavy data activity. This can be manifested as having unusually slow

Internet connectivity on all devices."

Earlier on, the SANS Institute had spotted the worm. SANS is a source for information security training and certification, and operates an Internet early warning system, the Internet Storm Center (ISC). The ISC issued an alert on February 12 about a suspected exploit in some Linksys routers. Johannes B. Ullrich, SANS Technology Institute, wrote in the InfoSec Handlers Diary blog on February 13: "We do not know for sure if there is a command and control channel yet. But the worm appears to include strings that point to a command and control channel. The worm also includes basic HTML pages with images that look benign and more like a calling card. They include images based on the movie 'The Moon' which we used as a name for the worm."

More information: isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633

Citation: Fixes in the works for Moon-struck Linksys routers (2014, February 18) retrieved 9 April 2024 from https://techxplore.com/news/2014-02-moon-struck-linksys-routers.html