Hewlett-Packard offers fix for printers susceptible to remote hacks

By Jeremy C. Owens   jowens@mercurynews.com

Posted: 12/23/2011 09:38:37 AM PST

Hewlett-Packard (HPQ) released a firmware update Friday that is says will fix a susceptibility in some of the Palo Alto company's popular LaserJet printers that researchers said could allow hackers to remotely take control of the devices.

Last month, MSNBC reported a team of researchers from Columbia University discovered that some Hewlett-Packard LaserJet printers, and possibly similar devices, did not verify software upgrades contained within so-called remote firmware updates. The researchers were able to offer firmware updates that included malicious software and then take control of the printer.

Once the researchers were able to take control of HP printers, they were able to accomplish a host of potentially dangerous tasks. They said they could print a tax return while sending a copy to a hacker's remote computer, compromising a host of personal information; easily disable printers; and even command a printer to continuously heat up its ink-drying component until it started to catch fire.

Hewlett-Packard issued a statement after the report was released vehemently denying that printers could be commanded to burst into flames and saying "no customer has reported unauthorized access," but the company did admit there was a flaw.

"HP has identified a potential security vulnerability with some HP LaserJet printers ... if placed on a public Internet without a firewall. In a private network, some printers may be vulnerable if a malicious effort is made to modify the firmware of the device by a trusted party on the network, " the statement read.

On Friday, HP issued a news release reiterating that no customers have reported unauthorized access to their LaserJet printers, and offered a firmware update that the company says will "mitigate this issue." The update is available at www.hp.com/support, in the "Drivers" category.

Researchers warned that if a hacker had gained control of a printer in this manner, however, there would be no way to reverse the process.

"If and when HP rolls out a fix, if a printer is already compromised, the fix would be completely ineffective. Once you own the firmware, you own it forever. That's why this problem is so serious, and so different," researcher Ang Cui said. "This is nothing like fixing a virus on your PC."

Hewlett-Packard recommends placing printers behind a firewall to protect exposure to remote hacks and disabling remote firmware upload capabilities on exposed printers.

http://www.mercurynews.com/ci_19608770?IADID=Search-www.mercurynews.com-www.mercurynews.com