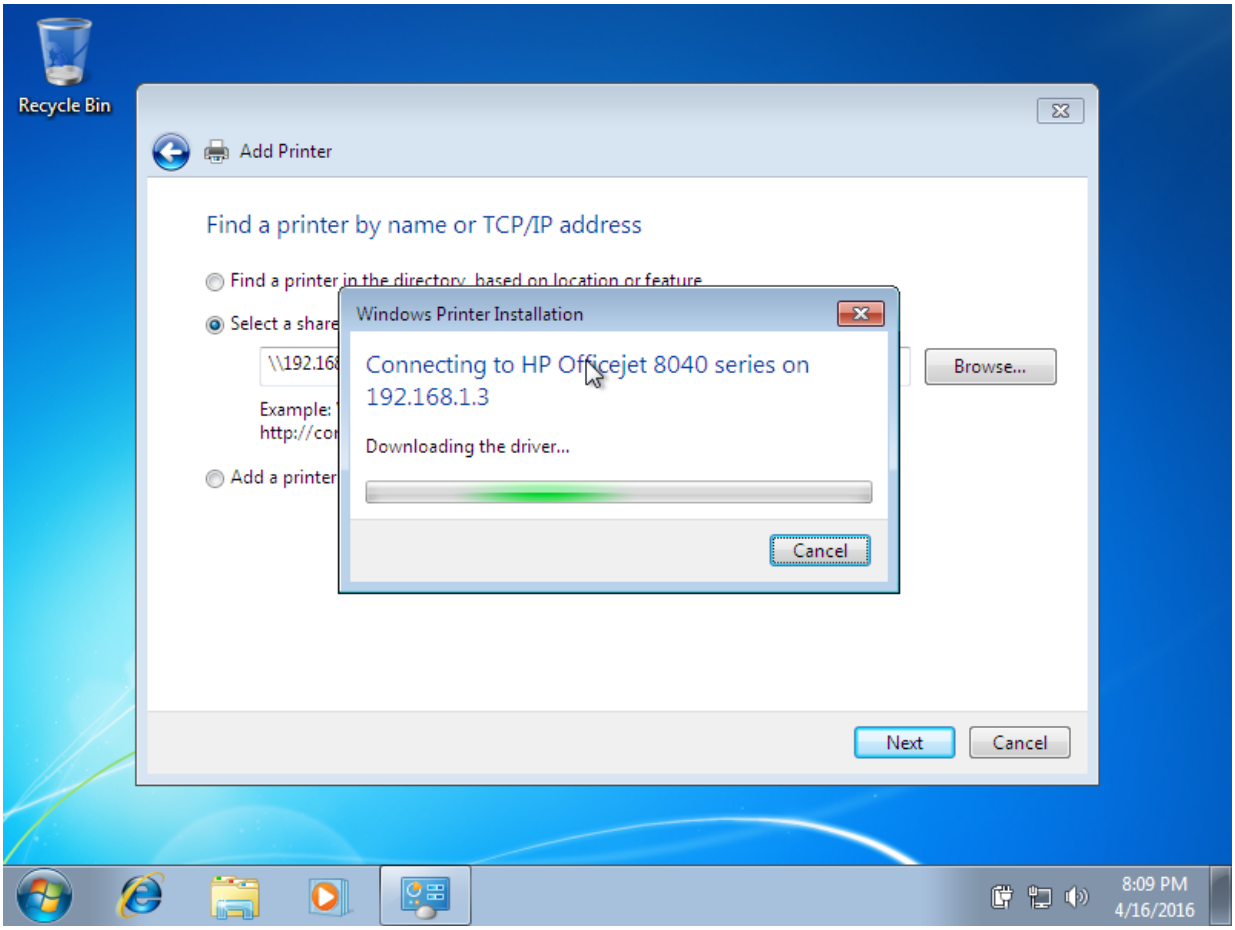
# Microsoft issues patch for print spooler-related vulnerability

July 14 2016, by Nancy Owano




(Phys.org)—Vectra Networks earlier this week revealed that their

researchers discovered a vulnerability in Microsoft Windows for an attacker to gain system-level control over computers via infected or fake printer drivers.

Tyler Lee in *Ubergizmo* wrote that after about 20 years, the Windows printer bug was discovered, turned out to be a vulnerability in the Windows Print Spooler software. Hackers could have been able to slip in malware because, said Lee, the spooler would not verify if the printer's drivers were the real deal.

Thankfully a patch was issued by Microsoft.

Vectra Networks security researchers said the vulnerability was affecting all versions of Microsoft Windows reaching all the way back to Windows 95.

The bug can only be taken advantage of if the attacker attaches the device to your PC or network. In the range of what can be tampered with, what are the chances of a stranger breaking in to your room just to do this type of thing? Possible but rather low.

OK, what about office settings?

Tyler Lee wrote that "What's worse is that if the printer is connected to a network, like in an office, it could potentially spread to other PCs on the same network as well, infecting all of them in the process."

Jon Fingas in *Engadget* commented: "The main saving grace: the attacker needs to attach the device to your PC or the local network. As such, the threat is mainly limited to public hotspots, loosely guarded office networks and other situations where someone could theoretically attach a rogue printer without drawing your attention."

Dan Goodin in *Ars Technica* also weighed in, writing that "code-execution attacks won't work in enterprise settings that use Microsoft's Active Directory unless administrators have modified default settings. Still, the attack is likely viable in many homes and small- and medium-sized businesses, especially those that allow people to connect their own devices."

Goodin quoted security expert HD Moore, who said, "This is mostly a risk for BYOD laptops within a company, folks using personal laptops on public networks, and corporate networks where the group policy explicitly enables this feature."

Wade Williamson of Vectra said earlier this week that "Vectra and Microsoft collaborated during the investigation of this issue, and Microsoft has delivered a fix as part of Security Bulletin MS16-087."

The update is titled "Security Update for Windows Print Spooler Components (3170005)" and it was rated as "Critical." What is the update all about? First of all, it corrects how the Windows Print Spooler service writes to the file system; it also issues warning to users trying to install untrusted printer drivers.

Goodin said the Vectra researchers tested their exploits on various devices that included "an unidentified printer and computers running Windows XP 32bit, Windows 7 32bit, Windows 7 64 bit, Windows 2008 R2 AD 64, Ubuntu CUPS, and Windows 2008 R2 64 print server."

Williamson advised organizations to pay attention to the fix: "As of 12 July 2016, Microsoft has provided a patch for this vulnerability as part of Security Bulletin MS16-087 and it is highly recommended that organizations apply the patch as soon as possible. It is also an example of the important role that IoT devices play in the security posture of the network. These devices can be hard to patch, hard to monitor and can

quickly become a persistent blind-spot for security operations. This is a good reason to monitor all of your internal traffic regardless of the device type."

In the bigger picture, printers should be part of security concerns:

"Printers present an interesting case in the world of IoT (Internet of Things), as they are very powerful hardware compared to most IoT devices, yet are not typically thought of as a 'real' computer by most administrators," said Nick Beauchesne in a Vectra analysis.

Josephine Wolff, an assistant professor of public policy and computing security at Rochester Institute of Technology, wrote in *Slate* in April: "Many printers these days are as technologically sophisticated—and vulnerable—as personal computers; they can connect to wireless networks and store data on hard drives. And the more sophisticated printing technology gets, the more complicated their security vulnerabilities can become."

**More information:** — http://blog.vectranetworks.com/blog/microsoft-windows-printer-wateringhole-attack
— https://technet.microsoft.com/library/security/MS16-087