HP Inc.
1501 Page Mill Road
Palo Alto, CA 94304

Hp.com

Security Advisory

HP Enterprise Printing Communication: WannaCry ransomware

June 2nd , 2017 (Revision History)

On Friday May 12, 2017, a ransomware called WannaCry (or WannaCrypt, WanaCrypt0r 2.0) began infecting systems around the world. The ransomware targets Windows SMB server using port 445 on Windows OS platforms. This ransomware has garnered a substantial amount of media attention. See the references section for links to additional resources describing WannaCry in detail.

At this time, we have completed investigations on the HP printing devices listed below. The listed HP printing devices are not vulnerable to this particular attack as they either do not support an SMB server or they are not running a Windows based operating system:

- HP LaserJet Enterprise printers and multifunction printers
- HP LaserJet printers and multifunction printers
- HP LaserJet Pro printers and multifunction printers
- HP PageWide Enterprise printers and multifunction printers
- HP PageWide Pro printers and multifunction printers
- HP Digital Senders and Document Capture Workstations
- HP OfficeJet Enterprise series printers and multifunction printers
- HP OfficeJet Pro printers and multifunction printers
- HP Envy series printers and multifunction printers
- HP Photosmart series printers and multifunction printers

- HP DeskJet series printers and multifunction printers

HP Software Solutions

HP Software Solutions rely on their host OS and are not directly involved. The attack occurs at the OS level and therefore patches or remediation recommendations should be followed from Microsoft®, the OS provider. The Microsoft® bulletin[2] states, "The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests".

The following solutions require the SMB protocol and leverage the host OS SMB services. SMBv1 can be disabled on the host server if the host OS supports SMBv2 or higher.

Note: Windows XP (or earlier) and Windows Server 2003 (and earlier) do not support SMB versions higher than SMBv1. Customers running these operating systems should apply the security patches released from Microsoft to allow SMBv1 availability to solutions.

- HP Access Control
- HP Capture & Route
- HP Security Manager
- HP Universal Print Driver
- HP Web Jetadmin
- HP Digital Sending Server
- Safecom
- Celiveo
- Equitrac

What can you do?

Subscribe to HP real-time security information: All HP products use a common centralized Security Bulletin process managed by HP´s Product Security Response Team (PSRT). Subscribe to HP Security Bulletins by following these steps:

1. Go to http://www.hp.com/go/support.
2. Click **Get software and drivers.**
3. Find your product.
4. Scroll to the bottom of the page and under **Other support resources**, click **Sign up for driver, support & security alerts**.

5. Follow the onscreen prompts to sign up for alerts.

References

1. https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

2. "Microsoft Security Bulletin MS17-010 – Critical"

Revision History

Revision	Date	Reason
1.0	16 - May - 2017	Initial Version
2.0	19 – May - 2017	Added HP PageWide Pro printers and multifunction printer
2.1	25 – May - 2017	Updated language regarding SMB servers
2.2	02 – June - 2017	Added Solutions and Windows server SMB support