opentext™

Fax Protocol Vulnerability “Faxploit”

OpenText response document

The Information Company

On **August 13, 2018**, Check Point Research published an article regarding a security flaw in HP all-in-one devices. According to HP, two security vulnerabilities affect certain HP Inkjet printers where a maliciously crafted file sent to an affected device can cause a stack or static buffer overflow, which could allow remote code execution. HP has updates available for download to address the vulnerability.

It is important to note that the security issue is isolated to the HP devices and is not related to the T.30 fax protocol as the article erroneously suggests. The vulnerability is specific to the operating system (OS) running on certain HP all-in-one devices and is not related to the T.30 fax protocol. The research firm used fax communication to inject malicious code on the HP device and exploit the HP OS but did not exploit the T.30 fax protocol. The researchers determined how to cause a buffer overflow on the HP device by sending a malicious .JPG file, knowing that the device’s OS would not check files received this way.

OpenText™, the most trusted provider of market-leading fax solutions, has determined that Check Point Research’s assertions that the T.30 fax protocol and other fax machines, fax servers, and fax services are vulnerable to this exploit are false. OpenText fax solutions, including on-premises, hybrid, cloud, and managed service solutions, and the T.30 protocol remain secure and trusted methods of communication across the globe.

OpenText has determined that none of our products or services are vulnerable to this exploit. Our fax hardware, software and services do not utilize the same OS as the HP devices and do not contain the same remote code execution vulnerability. Furthermore, the vulnerability existed only on HP devices running a ThreadX-based real-time OS by Green Hills. The assumption that this vulnerability extends to standalone fax machines, fax servers, fax-to-mail services, and other fax implementations is misleading. Rest assured, this vulnerability does not extend to any OpenText Fax Solutions.

Please visit our website to learn more about the most trusted and secure fax solutions available from the only fax solution provider with deployment options to fit every enterprise faxing need.

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX), visit opentext.com.

Connect with us:

OpenText CEO Mark Barrenechea's blog

Twitter | LinkedIn

opentext.com/contact