HealthManagement
Promoting Management and Leadership

Network security angst? Ditch your fax

Afraid of committing a security faux pas? Then it may be time to discontinue using those fax machines. New research from Check Point has uncovered a vulnerability in the ITU T.30 fax protocol that could be hacked to launch a cyberattack and gain access to a network.

Based on Check Point's "Faxploit" research, fax machines can be hacked to breach a network – using only its number. The hacker could simply send a malformed fax image to the fax machine with a code that will exploit a flaw in two buffer overflows in the protocol components that handle DHT and COM markers.

In so doing, the hacker could then gain remote code execution rights on the device, which would let them run malicious code and take over the fax machine. They would then be able to download and deploy other tools to scan the network and compromise devices.

At this year's DEF CON, Check Point researchers demonstrated how an attacker could easily compromise a fax machine to download and launch the EternalBlue exploit, which is able to infect all nearby computers exposed by the SMB protocol. This attack method was used in both Petya and WannaCry. As the researchers noted in their presentation, the exploit doesn't require an internet connection, just a phone line.

Considering that Google indexed more than 300 million fax numbers, experts warned hackers could target almost any organisation. There are no security tools that scan incoming faxes, meaning that prevention of the faxploit is almost impossible. The researchers said organisations must patch the flaw on individual fax devices and all-in-one machines with embedded faxes to block unauthorised access.

These problems highlight the importance of segmenting a network – even, especially, fax machines.

"Due to the high operational demands placed on a business, most enterprises overlook many IT security practices and lack properly defined segmentation policies," the report authors wrote. "This means that once a threat actor has penetrated your perimeter defences, they can roam freely within your network."

"If you do not want to disconnect your printer-fax machine, then at least make sure it is placed in a segmented area," they continued. "By doing this, even if it does become compromised the attacker will not be able move laterally and infect other parts of your IT network."

The researchers used an HP all-in-one printer/fax machine, although the vulnerability is found in the fax protocol itself. Check Point worked with HP to make sure the product received a patch for the vulnerability, but other fax machines may still have the flaw.

Security researchers have long bemoaned the use of fax machines, as the antiquated devices pose real privacy issues when it comes to transmitting patient data. It is estimated that 75 percent of all healthcare communications are still processed by fax.

And while Centers for Medicare and Medicaid Services Administrator Seema Verma recently called for an end to provider fax machines by 2020, this newly discovered cybersecurity vulnerability suggests that plenty of networks could be at risk from the exploit over the next two years.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Wed, 22 Aug 2018