Security Advisory Report - OBSO-1808-01

Faxploit: DEF CON 2018: HP OfficeJet Printer Attack (CVE-2018-5925,CVE-2018-5924)

Creation Date:	2018-08-20 16:18:37
Last Update:	2018-08-22 11:19:58

Summary

DEF CON 2018: Critical Bug Opens Millions of HP OfficeJet Printers to Attack

Fax-ready HP OfficeJet inkjet printers are vulnerable to a hack that gives an attacker full control over a targeted printer.
Once compromised, the all-in-one OfficeJet could act as a springboard for deeper network penetration by an attacker.

A malicious fax sent to an HP Inc. OfficeJet all-in-one inkjet printer can give hackers control of the printer and act as a springboard into an attached network environment.

After the malicious fax a huge XML (> 2GB) file was sent to the printer over TCP port 53048 thus triggering a stack-based buffer overflow.

The vulnerability is tied to all-in-one printers that support Group 3 (G3) fax protocols, part of the ITU T.30 standard for sending and receiving colour faxes.

The hack is specific to HP OfficeJet inkjet printers. It required considerable research, debugging and specific exploits.

It will not work on other Fax devices.

In general we believe there are easier ways to compromise a corporate network, even if there's such an HP fax-printer in there; the novelty of this vector is that they got in via a plain analog phone line.

https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/

Details

This attack, although it uses the T30 protocol elements to find out how the printer software was constructed, is very specific.

ARM 32bit CPU, ThreadX-based real-time Operating System by Green Hills are used by HP.

A long and tedious research was done reversing the T.30 state machine and later reversing the task that handles the HDLC modem.
A showcase for DEF CON 2018 was created using Eternal Blue to exploit PCs connected.

A HW debugger was hooked into the machine to learn about internal SW.
Buffer overflow attacks with exploit is usually a very specialized attack for a specific target, because the attack needs to be binary compatible with the specific SW and it´s vulnerabilities.

Xpressions is **not** vulnerable to **this** attack. The attack works by sending a JPEG-encoded fax to an all-in-one printer and exploiting a bug in its proprietary JPEG decoding module.
Xpressions does not support receiving JPEG encoded fax messages, and it would not try to JPEG-decode such a fax.

They used a flaw in a jpeg library that HP uses when receiving color faxes. None of this applies to Unify products.

Although such reverse engineering techniques could theoretically be used on the Unify Fax Stack, hackers would need to start research from scratch and develop a completely new attack.

Affected Products

This "faxploit" attack is specific for HP OfficeJet Printers.

Unify does not sell HP OfficeJet Printers.

No Unify product is affected.

Recommended Actions

No Unify product is affected, no action necessary.

References

https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/

https://threatpost.com/def-con-2018-critical-bug-opens-millions-of-hp-officejet-printers-to-attack/134972/

https://www.heise.de/security/meldung/Totale-Kontrolle-Multifunktions-Drucker-ueber-Fax-angreifbar-4135522.html https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/

https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/

https://thehackernews.com/2018/08/hack-printer-fax-machine.html

Advisory: OBSO-1808-01, status: draft
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.