Dialogic Position on Check Point Software Technologies' "Findings" on Fax Vulnerabilities

Background

On August 13, 2018, Check Point Software Technologies Ltd. issued a press release that discussed what in its view were vulnerabilities and potential security risks in fax devices. This research was specific to the HP Officejet Pro All-in-One printer and related solely to the parsing of JPEG files, that had been sent via fax, using a proprietary JPEG parser to interpret the fax data. The vulnerability in the HP Officejet Pro All-in-One printer ("HP Device") has been addressed via a patch available from HP, and is discussed in this HP Security Bulletin. The press release issued by Check Point Software Technologies also suggested that other fax devices and services could share this vulnerability; however, no known issues outside of this research have been reported, as stated in Check Point's Research Blog.

Considerations for Solutions Based on Dialogic® Brooktrout® Fax Software

Fax servers and other solutions based on Brooktrout Fax software use the T.30 fax protocol as the underlying transport for sending and receiving real-time faxes over IP or TDM networks. The vulnerability described in the Check Point press release did not reside in the T.30 transport, but rather on the receiving side and the way it handled data it received. The situation is akin to malicious code being sent via an email in that the medium by which transport occurs is not where the vulnerability lies.

In more detail, the Check Point press release and its related blog indicate that Check Point was able to reverse engineer HP Officejet Pro All-in-One printer firmware code that handles JPEG color fax images to force a stack overflow and allow execution of a malicious attack. In such a scenario, a calling party sent a fax, containing malicious code, in JPEG file format to the HP Device via a fax session using the T.30 protocol. The HP Device then used a proprietary JPEG parser to interpret the fax data. The vulnerabilities with this custom JPEG parser were related to stack-based buffer overflows. As stated in the HP Security Bulletin: "a maliciously crafted file sent to an affected device can cause a stack or static buffer overflow, which could allow remote code execution." Because the HP Device uses an embedded real-time operating system, Thread X-based, running in kernel-mode using a flat memory model, the malicious file would then have access to the Ethernet, LCD and all components of the HP Device.

The use of a JPEG file to exploit the vulnerabilities in the HP Device was key, due to the use of HP's proprietary JPEG parser. By default, the Brooktrout API restricts the receiving of JPEG files.

In addition, Brooktrout-based fax solutions should not be subject to the same vulnerability described in the Press Release because they work only on Windows and Linux platforms. Generally speaking, the Windows and Linux operating systems' architectures, and how they execute code, help prevent automatic execution of malicious code, regardless of how the code is sent to a particular machine.

Summary

Dialogic Inc. 4 Gatehall Drive, Parsippany, NJ 07054 USA **Tel:** +1.973.967.6000 **Fax:** +1.973.967.6006

Based on information available as of August 16, 2018, Brooktrout fax products would not be vulnerable to a similar attack. The vulnerability described by Check Point is not related to the T.30 protocol. That does not mean similar vulnerabilities do not exist in any non-Brooktrout fax solution; but that if fax protocols and other best practices are followed, this type of attack should not occur.

Recommended Action

It is recommended that users apply all recommended updates for their fax, network, and other components in line with their applicable security policy/policies and as recommended by all manufacturers. As always, Dialogic suggests maintaining appropriate security access and policies to prevent unwarranted access to systems to reduce the chance of a malicious agent accessing systems and installing a program that could take advantage of the security exploit.

References:

Check Point Software Technologies Ltd Press Release
https://www.checkpoint.com/press/2018/faxploit-new-check-point-research-reveals-criminals-can-target-company-private-fax-machines-take-networks-spread-malware/

Check Point's Research Blog
https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/

HP Security Bulletin
https://support.hp.com/us-en/document/c06097712

Dialogic Inc. 4 Gatehall Drive, Parsippany, NJ 07054 USA **Tel:** +1.973.967.6000 **Fax:** +1.973.967.6006