Security Advisory Report - OBSO-1704-01

Microsoft Patchday March 2017: Microsoft Windows SMB Remote Code Execution vulnerabilities

Creation Date: 2017-04-28
Last Update: 2017-05-09

Summary

Microsoft Patchday March 2017 revealed several SMB vulnerabilities.

This security update resolves vulnerabilities in Microsoft Windows.
The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated critical for all supported releases of Microsoft Windows.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

These vulnerabilities affect Microsoft only, since SMB is a Microsoft specific SW.

https://en.wikipedia.org/wiki/Server_Message_Block

Linux is not affected

Vulnerability Details

Microsoft Security Bulletin MS17-010 - Critical
Security Update for Microsoft Windows SMB Server (4013389)

Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.

To exploit the vulnerability, in most situations, an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server.

For installations in an isolated environment that are not reachable from the internet priority can be reduced.

The security update addresses the vulnerabilities by correcting how SMBv1 handles these specially crafted requests.

https://technet.microsoft.com/library/security/ms17-010

https://support.microsoft.com/en-us/help/4013078/title

CVE-2017-0143

CVE-2017-0144

CVE-2017-0145

Microsoft Windows SMB Server Request Handling Unspecified Remote Code Execution

Microsoft Windows contains a flaw in the Server Message Block 1.0 (SMBv1) server that is triggered during the handling of certain requests. With a specially crafted packet, a remote attacker can potentially execute arbitrary code.

CVE-2017-0146

CVE-2017-0147

Microsoft Windows SMB Server Request Handling Unspecified Remote Code Execution (ETERNALCHAMPION)

Microsoft Windows contains a flaw in the Server Message Block 1.0 (SMBv1) server that is triggered during the handling of certain requests. With a specially crafted packet, a remote attacker can potentially execute arbitrary code.

CVE-2017-0148

Microsoft Windows SMB Server Request Handling Unspecified Remote Code Execution

Microsoft Windows contains a flaw in the Server Message Block 1.0 (SMBv1) server that is triggered during the handling of certain requests. With a specially crafted packet, a remote attacker can potentially execute arbitrary code.

Tool to check if MS17-010 has been patched from remote.

https://www.exploit-db.com/exploits/41891/

https://packetstormsecurity.com/files/142181/Microsoft-Windows-MS17-010-SMB-Remote-Code-Execution.html

https://github.com/countercept/doublepulsar-detection-script

NSA exploits:

https://github.com/fuzzbunch

https://www.dearbytes.com/blog/playing-around-with-nsa-hacking-tools/

Affected Products

OpenScape Xpert is affected in case the Windows version of the turret 6010p is used

OpenStage Xpert 6010p turret (Windows) V5 R1
OpenStage Xpert 6010p turret (Windows) V5
Turrets: use V5 R1.5.5 or later

Recommended Actions

1.) OpenStage Xpert 6010p (Windows)

As V5 is phased-out, please consider upgrading to a supported version V5 R1.5.5 or later as soon as possible where the corrective measure is available.

Update the OS of the OpenStage Xpert 6010p devices as described in the Service Manual (chapter 8.8).

All relevant patches from April 2017 and earlier are included.

2.) Products that are delivered as applications by Unify:

This Microsoft patch should be installed per the standard process for applying Microsoft Windows patches

For affected Windows versions and a workaround see:

https://technet.microsoft.com/library/security/ms17-010

References

https://technet.microsoft.com/library/security/ms17-010

https://support.microsoft.com/en-us/help/4013078/title

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-0143

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-0144

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-0145

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-0146

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-0147

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-0148

Revision History

First draft 2017-04-26

Released 2017-04-28

Updated 2017-05-09

Advisory ID: OBSO-1704-01 (a=162), status: general release
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