Security Advisory Report - OBSO-1412-01

Microsoft Windows Remote Code Execution Vulnerability in Schannel ("Winshock", MS14-066, CVE-2014-6321)

Creation Date: 2014-12-01
Last Update: 2015-06-16

Summary

On Nov. 11, 2014 Microsoft has issued the security advisory MS14-066 that discloses a vulnerability in the Security Channel (Schannel) component, affecting all Microsoft Windows (server and client) operating systems. The vulnerability is also known as "Winshock".

The risk is rated as **high**.

This advisory describes the associated mitigation measures and solutions for Unify products based on Windows (client or server), especially for the trading device **OpenStage Xpert 6010p**.

Vulnerability Details

Schannel provides a set of cryptographic functions and security protocols. It is used by many applications and services on both Windows server and Windows client operating systems.
The vulnerability could allow remote code execution with administrative privileges on the target Windows system: an attacker could send specially crafted packets to a service on that system that relies on the vulnerable schannel component.
Potentially vulnerable services include but are not limited to the Microsoft IIS webserver, RDP (remote desktop protocol), MS SQL, LDAPS and many other applications that support the SSL/TLS protocol on Windows systems.
For more details refer to Microsoft's security advisory MS14-066.

CVSS Scores:

- Base Score: 9.3, Temporal Score: 9.3
- CVSS v2 Vector (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:H/RL:U/RC:C)

Mitre (cve.mitre.org) has assigned CVE-2014-6321 to this issue.

Affected Products

- OpenStage Xpert 6010p, all versions **before V5 R0.3.0**
- All Microsoft Windows servers (Server 2003, 2008, 2008 R2, 2012, 2012 R2) and clients (Vista, 7, 8, 8.1)
  Note: older versions (such as Windows Server 2000 or Windows XP) have already achieved end of SW support, but may also be affected

Recommended Actions

1. OpenStage Xpert 6010p (Turret)

The Trading devices (turrets) are based on Windows XP-embedded and are vulnerable via the RDP protocol.
Solution available: update to V5 R0.3.0 (release date 2015-06-11 (*)) or later.

The following mitigations exist for unpatched versions of OpenStage Xpert. These are general hardening recommendations and are therefore also recommended in installations where V5 R0.3.0 or higher has already been applied:

- If not used/needed: disable the RDP protocol on all turrets
- Use the Group Policy Management on the Domain controller to enable Windows XP firewall settings on all turrets and restrict the remote desktop access to relevant systems (System Manager, MLC) only; a detailed description, including a comprehensive list of recommended firewall settings is available through your support contact at Unify.

(*) Note that OpenStage Xpert V5 R0.3.0 also includes additional (but less relevant) Windows XP security fixes:

- MS15-028 - Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377) - CVE-2015-0084
- MS15-016 - Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3029944) - CVE-2015-0061
- MS15-014 - Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361) - CVE-2015-0009

- MS15-010 - Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220) - CVE-2015-0003
- MS15-003 - Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674) - CVE-2015-0004
- MS14-067 - Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958) - CVE-2014-4118

2. All Microsoft Windows servers and clients

The associated solution for Schannel is described in Microsoft's knowledge base entry KB2992611. We recommend all customers to apply the patch (*along with other relevant patches published at the same patch day - Nov. 11, 2014*) to any Microsoft Windows server or client, including those where Unify applications are installed and operated on. No incompatibility issues with Unify products are known.
Note that KB2992611 was updated by Microsoft on Nov. 18 to provide new patches for Windows Server 2008 R2 and Windows Server 2012. They solve compatibility problems with the new cipher suites introduced with the initial patches (as of Nov. 11). Microsoft therefore recommends to reinstall the patch.

References

Microsoft:

- Security Advisory MS14-066
- Knowledge Base article KB2992611
- Additional Advisories and Knowledge Base articles as referenced in chapter "Recommended Actions"

Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6321

US-Cert: https://www.us-cert.gov/ncas/alerts/TA14-318A

Revision History

2014-12-01: Initial release
2015-06-16: Update 01

- Fix release available for OpenStage Xpert 6010p (V5 R0.3.0)
- Added information about additional (but less relevant) security fixes included in the same release

---

Advisory ID: OBSO-1412-01 (a=97), status: update 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