Security Advisory Report - OBSO-1404-02-A

Appendix: Impact of the "Heartbleed" vulnerability (CVE-2014-0160) to third-party products

Creation Date: 2014-04-18
Last Update: 2014-05-02

Summary

This is not a separate Unify Security Advisory, but an appendix to the advisory OBSO-1404-02.

Vulnerability Details

Solutions from Unify may use or be based on various products from other vendors ("third-party products"), that are not included in the core Unify product portfolio, such as network components, operating systems, video systems or security applications. These products are not monitored as part of Unify's Vulnerability Intelligence Process and are therefore also not covered by the Unify Security Advisory OBSO-1404-02. However, for your additional support we have collected important information about the impact of CVE-2014-0160 to these systems in this appendix.

Affected Products

Operating Systems and Virtual Machines:
- Microsoft (not affected):
- Novell SLES (versions used by Unify are not affected):

Hardware and associated tools:
- Fujitsu:
  Note: this link requires Fujitsu partner login; Unify-related summary of the current information:
  - iRMC (IPMI) or other Fujitsu software is not affected, only: ServerView RAID Manager 5.5, 5.6, 5.7; fix release plans and mitigation information available in the advisory from Fujitsu
  - No direct impact to Unify solutions, provided that ServerView RAID Manager is only used at initial installation/staging time to setup the RAID system, as it applies to e.g. OpenScape Voice in standard installation procedures.

Networking:
- Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

3rd-party Voice and Video Systems:
- Lifesize: http://www.lifesize.com/~media/Documents/Related%20Resources/Heartbleed%20Bug%20Additional%20Information.ashx
Security applications and devices:

- **TrendMicro** (used in Antivirus for OpenScape Servers):
  - See chapter "Recommended Actions" for details regarding the impacts to Antivirus for OpenScape Servers


- **Bluecoat**: [https://kb.bluecoat.com/index?page=content&id=SA79](https://kb.bluecoat.com/index?page=content&id=SA79)


- **HP Tipping Point**: see Advisory link in the Networking section above (Hewlett-Packard)


- **Imprivata OneSign**: No official vendor statement available. Our assumption however is that it is not affected, since the OneSign appliance is delivered with a non-vulnerable version of OpenSSL.

Further technology partners:

- **ATOS** (DirX Product Portfolio): [https://iam-support.it-solutions.atos.net/rss/rss.php?cat=1](https://iam-support.it-solutions.atos.net/rss/rss.php?cat=1)
  - DirX Directory and DirX Identity are affected; DirX Access / DirX Audit probably not affected.
  - See also [OBSO-1404-02](https://kb.bluecoat.com/index?contentId=SA79) regarding the impact of DirX Directory to OpenScape Identity and Lifecycle Assistant (OS ILA).

- **MSI TeleSolutions** (TeleData, HospiX product line etc.): no product is affected

- **Aurenz GmbH** (Alwin Pro, Annad etc.): no product is affected

- **Beyertone GmbH** (musiphone product line etc.): no product is affected

- **C4B Com for Business** (Xphone product line): no product is affected


**Recommended Actions**

We recommend to check the third-party vendor information for potential updates regularly, and wherever possible subscribe to the corresponding vendor's advisory alert service.

Unify's product security team does not control or guarantee the currency, accuracy, or completeness of information found on the linked, external sites. If you need additional assistance, please contact your Sales or Services representative at Unify.

**Additional information for TrendMicro products:**

In the context of the Unify solution “Antivirus for UC Servers”, the following products of TrendMicro are affected, appropriate fix releases or patches are available:

**Deep Security**


- Deep Security Manager (DSM), Deep Security Agent (DSA), and Deep Security Virtual Appliance (DSVA) components are not affected.

  Also, Deep Security 7.5 is not affected since it does not have Deep Security Relay.

**Server Protect**

- **Server Protect for Linux** (SPLX) is affected.
  
  
  For use on Unify UC Application servers this critical patch was included in the latest SPLX release package (version r23, release date 2015-04-25).
  
  You can retrieve the patch through your regular support channel or at Trend Micro download center directly: [http://files.trendmicro.com/products/patches/splx_30_lx_en_criticalpatch1414.tar.gz](http://files.trendmicro.com/products/patches/splx_30_lx_en_criticalpatch1414.tar.gz)
  
  To update an existing SPLX installation, use the "latestpatchonly" package.
  
  The "full" package is only required for systems where SPLX is currently not installed.

- **Server Protect for Windows** (SPNT) is not affected.

**Control Manager (TMCMD)**: The Control Manager (Version 5.5, 6.0, 6.0 SP1, Standard and Advanced) is not affected.
References

- Unify Security Advisory OBSO-1404-02

Revision History

2014-04-18: Initial release

2014-04-23: Update 01:
- New/updated information for various vendors (highlighted appropriately with "new"/"updated"): Extreme Networks, Imperva, Imprivata, Fujitsu, ATOS, MSI Solutions

2014-04-25: Update 02:
- New information for vendor: Aurenz GmbH

2014-05-02: Update 03:
- New/updated information for vendors: Beyertone, C4B, Trendmicro (incl. relevance to Antivirus for OpenScape Servers)
- Minor adaptations in wording

Advisory ID: OBSO-1404-02-A (a=80), 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
© Unify Software and Solutions GmbH & Co. KG 2014
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.