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):
  http://blogs.technet.com/b/security/archive/2014/04/10/microsoft-devices-and-services-and-the-openssl-heartbleed-vulnerability.aspx
- Novell SLES (versions used by Unify are not affected):
  http://support.novell.com/security/cve/CVE-2014-0160.html
- VMWare: http://kb.vmware.com/kb/2076225 and http://www.vmware.com/security/advisories/VMSA-2014-0004.html

Hardware and associated tools:

- Fujitsu:
  https://partners.ts.fujitsu.com/com/news/Pages/Heartbleed.aspx#solutions
  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:

- Extreme Networks/Enterasys: http://esupport.extremenetworks.com/ and http://go.extremenetworks.com/641VMV6020004sk000Zcf00
- Cisco: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed
- Hewlett-Packard: http://h17007.www1.hp.com/docs/advisories/HPNetworkingSecurityAdvisory-OpenSSL-HeartbleedVulnerability.pdf
- Infoblox (not affected): https://community.infoblox.com/blogs/2014/04/14/infoblox-statement-about-openssl-heartbleed-defect

3rd-party Voice and Video Systems:

- Polycom: http://www.polycom.com/content/dam/polycom/common/documents/brochures/heartbleed-security-advisory-enus.pdf
- Cisco (incl. Tandberg): http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed
- 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):
  - Overview for all TrendMicro products: http://esupport.trendmicro.com/solution/en-US/1103084.aspx
  - **See chapter "Recommended Actions" for details regarding the impacts to Antivirus for OpenScape Servers**

- Fortinet (used in OpenScape UC Firewall): http://www.fortiguard.com/advisory/FG-IR-14-011/
- F5 Networks (F5 BIG-IP): http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15159.html?sr=36517217
  and https://devcentral.f5.com/articles/openssl-heartbleed-cve-2014-0160
- Bluecoat: https://kb.bluecoat.com/index?page=content&id=SA79
- Checkpoint: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk100173
- HP Tipping Point: see Advisory link in the Networking section above (Hewlett-Packard)
- Imperva:
  http://www.imperva.com/resources/adc/adc_advisories_response_heartbleed_CVE-2014-0160.html
- 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
  - DirX Directory and DirX Identity are affected; DirX Access / DirX Audit probably not affected.
  - See also OBSO-1404-02 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
  Overview of actively supported products: http://www.msi-telesolutions.com/en/support.php
- Aurenz GmbH (Alwin Pro, Anna4 etc.): no product is affected
- Beyertone GmbH (musiphone product lines etc.): no product is affected
- C4B Com for Business (Xphone product line): no product is affected
  Details:
  http://www.c4b.de/de/aktuelles/pressemitteilungen/2014/Heartbleed-OpenSSL-Bug--XPhone-Loesungen-von-C4B-sind-sicher.php

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 Relay (DRS) for Windows (Details: http://esupport.trendmicro.com/solution/en-US/1103268.aspx)
  - Patch information for Deep
    Security Relay v8.0: http://files.trendmicro.com/documentation/readme/DSR_8_0_SP2_P2_Build_2207_CriticalPatch_Readme.txt
  - Patch information for Deep
    Security Relay v9.0: http://files.trendmicro.com/documentation/readme/DSR_9_0_SP1_P2_Build_3335_CriticalPatch_Readme.txt
- 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.
  Details see http://files.trendmicro.com/documentation/readme/splx_30_lx_en_criticalpatch1414_readme.txt
  - 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
    - 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 (TMCM): 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

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