Security Advisory Report - OBSO-1406-01

openSSL ChangeCipherSpec Injection Vulnerability (CVE-2014-0224) and FLUSH+RELOAD Cache Side-channel Attack (CVE-2014-0076)

Creation Date: 2014-06-06
Last Update: 2015-07-28

Summary

On June 5th, 2014, the OpenSSL team published a security advisory containing several vulnerabilities. Among these vulnerabilities, only CVE-2014-0224 is relevant to the Unify product portfolio and may enable an attacker to perform man-in-the-middle (MITM) attacks against certain TLS connections in Unify/OpenScape solutions. The risk is rated as medium.

Additionally, CVE-2014-0076 (FLUSH+RELOAD cache side-channel attack against ECDSA nonces) potentially affects one product only (OpenScape Voice). The risk is rated as low.

Unify products are not affected by all other reported vulnerabilities (CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-3470).

Vulnerability Details

1. CVE-2014-0224 (openSSL ChangeCipherSpec Injection Vulnerability):

With regard to the ChangeCipherSpec vulnerability, openSSL does not properly restrict processing of ChangeCipherSpec messages, which allows MITM attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake.

Mitre (cve.mitre.org) has assigned the id CVE-2014-0224 to this issue.
CVSS v2 Base Score for Unify products: 6.8 (AV:N/AC:M/AU:N/C:P/I:P/A:P)

For a potential attack to be successful, both the server and the client in a TLS connection (such as https, SIP-TLS, HFA-TLS etc.) have to be vulnerable, i.e. both must use a vulnerable version of openSSL.
Therefore, the impact analysis below focuses on TLS connections used within Unify solutions, not on single products.

2. CVE-2014-0076 (Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack):

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

TLS connections from, to or between products of Unify are not affected, since ECDSA ciphers are not used or offered when TLS connections are established.
However, existing installations of **OpenScape Voice** are potentially vulnerable. A local attacker (logged on using ssh onto the OpenScape Voice appliance) may get access to another ssh session's memory on the same appliance and potentially determine the other ssh session's key.

Mitre (cve.mitre.org) has assigned the id CVE-2014-0076 to this issue.
CVSS v2 Base Score: 2.4 (AV:L/AC:H/Au:S/C:P/I:P/A:N)

Affected Products

1. CVE-2014-0224:

The following TLS connections are potentially vulnerable:

- **OpenScape Voice, OpenScape Branch, OpenScape SBC: SIP-MTLS trunk connections to third-party softswitches** may be affected, in case the third-party softswitch is confirmed as vulnerable. In such configurations please check also the third-party vendor's statement regarding CVE-2014-0224.

- **OpenStage and OpenScape Desk Phone IP phones are potentially affected in two TLS connections**:
    - SIP-TLS connections to third-party softswitches, in case the third-party softswitch is confirmed as vulnerable. In such configurations please check also the third-party vendor's statement regarding CVE-2014-0224.
    - When https (instead of FTP) is used for file and software deployment and the https server is vulnerable (for example an Apache httpd web server installed on Microsoft Windows Server, bundled with a vulnerable version of openSSL). In such configurations please update the https server's openSSL module accordingly.

This advisory will be updated, as soon as update releases for the affected products of Unify are available that will solve this issue independent of the status in any third-party softswitch and/or https server.
See also below for recommended precautionary measures, independent of the real impact of this vulnerability.

Available Software Releases that provide a correction for CVE-2014-0224
(incl. associated openSSL vulnerabilities as documented in https://www.openssl.org/news/secadv_20140605.txt):

- OpenScape Voice: Solution available: update to
    - V6 R0.2.0 (P30310-Q3044-Q160-02-7620, release date 2014-09-09), or
    - V7 R1.40.5 (release date 2014-08-27), or
    - V8 R0.26.5 (release date 2014-09-04)
- OpenScape Branch: Solution available: update to
    - V7 R1.20.0 (release date 2014-07-31), or
    - V8 R0.4.0 (release date 2014-08-14)
- OpenScape SBC: Solution available: update to
    - V7 R1.20.0 (release date 2014-07-31), or
    - V8 R0.4.0 (release date 2014-08-08)
- OpenStage / OpenScape Desk Phone IP HFA: update to
    - V3 R0.18.0 (release date 2014-09-18)
- OpenStage / OpenScape Desk Phone IP SIP: update to
    - V3 R3.24.0 (release date 2014-10-10)

TLS connections confirmed as not vulnerable are:

- **SIP-TLS and HFA-TLS connections (Internet/Intranet)** between end-user devices / applications: OpenStage and OpenScape Desk Phone IP VoIP phones, OpenScape Mobile, OpenScape Personal Edition
  and Unify communication platforms: OpenScape Voice, HiPath 4000 V6 / OpenScape 4000 V7 (incl. internet connections to 4000 Softgate), OpenScape Branch, OpenScape Session Border Controller (SBC), RG8700 and RG8300/RG8350a Gateways.
- **https for Web-based access** to management applications, web-based management interfaces provided by any Unify product or device: the list of released browsers is typically restricted to (a subset of): Microsoft Internet Explorer, Mozilla Firefox, Google Chrome.
  https connections using these browsers are not affected.
- The connection between **OpenScape Deployment Service** and VoIP Phones, Clients or Gateways (aka "DLS-WPI")

2. CVE-2014-0076:

- **OpenScape Voice**
  Corrections have been provided in alignment with CVE-2014-0224 (see 1.)

Recommended Actions

1. CVE-2014-0224:

The following recommendations are relevant not only as precautionary measures for CVE-2014-0224, but to reduce the likelihood of successful attacks against TLS connections in your solutions in general:

- For web-based access, avoid using Web Browsers, that are not released for use with Unify products
- Design and operate your IP network in a way that reduces the potential for man-in-the-middle (MITM) attacks in TLS connections, such as:
    - Segregation of networks, zoning, VLANs
    - Operation of firewalls, SBCs and configuration of access control lists
    - Physical access security to network elements
    - Use of the capabilities of network elements regarding protections against ARP spoofing, VLAN hopping and similar

2. CVE-2014-0076:

- Consider the hardening recommendations as documented in the Security Checklist for OpenScape Voice
- Ensure that the access to the ssh port and login to the appliance is limited to the operational and organisational needs and only granted to authorized and trusted personnel

3. General recommendation:
Although not rated as affected - further products of Unify will be updating their embedded version of openSSL as part of continuous maintenance and fix release activities. Specific product versions and release dates will be added to this advisory as appropriate. It is recommended to update to these versions as soon as available.

The following Unify products have included the appropriate updates of openSSL:

- OpenScape Xpressions V6 R2.7.17702 (release date 2014-07-08)
- OpenScape Business V1 R3.1.0 (release date 2014-08-18)
- OpenScape Accounting V1 R2.16.0 (release date 2014-09-30)
- OpenScape Office V3 R3.11.0 (release date 2014-10-17)
- OpenStage Diagnostic Data Collector V4 R3.11.0 (release date 2014-10-22)
- OpenScape Xpressions V7 R1.3.17883 (release date 2014-10-23)
- OpenScape Voice Trace Manager V8 R0.1.3 (release date 2014-12-10)
- HiPath 4000 Manager V6 R2.51.0 (release date 2014-12-16)
- OpenScape Contact Center Agile/Enterprise V8 R2.10.120 (release date 2014-12-18)
- HiPath 4000 V6 R2.17.1 (HF003973, release date 2014-12-19)
  incl. HiPath 4000 Assistant V6 R2.51.0 (release date 2014-12-16)
  and HiPath 4000 CSTA V1 R13 (release date 2014-11-25)
- OpenScape 4000 V7 R1.39.0 (release date 2015-05-29)
  incl. OpenScape 4000 Assistant V7 R1.7.5 (release date 2015-03-18)
  and OpenScape 4000 CSTA V7 R1.206.5 (release date 2015-04-24)
- **OpenScape Contact Center CDSS V8 R2.10.11192 (release date 2015-07-24)**

References

External links:

- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224 and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0076
- NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224 and http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0076
- openSSL: https://www.openssl.org/news/secadv_20140605.txt
- Description of the CCS injection vulnerability: http://ccsinjection.lepidum.co.jp/

Revision History

2014-06-06: Initial release

2014-07-11: Update 01:

- CVE-2014-0224: Added descriptions for potentially affected TLS connections between products of Unify and third-party systems
- Added information about CVE-2014-0076

2014-08-06: Update 02:

- Fix releases available for OpenScape Branch V7 and OpenScape SBC V7

2014-08-27: Update 03:

- Fix releases available for OpenScape Branch V8, OpenScape SBC V8 and OpenScape Business

2014-09-18: Update 04:

- Fix releases available for OpenScape Voice, OpenStage/OpenScape Desk Phone IP (HFA) and OpenScape Xpressions V6

2014-10-10: Update 05*:*

- Fix releases available for OpenStage / OpenScape Desk Phone IP (SIP) and OpenScape Accounting

2014-10-23: Update 06

- Fix releases available for OpenScape Office, OpenStage Diagnostic Data Collector, OpenScape Xpressions V7

2014-12-23: Update 07

- Fix releases available for OpenScape Voice Trace Manager, OpenScape Contact Center Agile/Enterprise, HiPath 4000 V6 R2, HiPath 4000 Manager V6 R2

2015-05-29: Update 08

- Fix release available for OpenScape 4000 V7 R1
- Added missing release information for CSTA in HiPath 4000 V6 R2

2015-07-28: Update 09

- Fix release available for OpenScape Contact Center CDSS V8 R2

Advisory ID: OBSO-1406-01 (a=82), 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