Security Advisory Report - OBSO-1512-01

OpenScape Voice - MTLS-SIP Denial of Service Vulnerability in OpenSSL Certificate Verification (CVE-2015-0286)

Creation Date: 2015-12-23
Last Update: 2015-12-23

Summary

Certain releases of OpenScape Voice V7 and V8 are vulnerable to Denial of Service (DoS) at the SIP interface if MTLS (TLS with mutual client and server authentication using X.509v3 certificates) is configured.

The risk is rated **medium**.

The issue is caused by a vulnerability in the ASN1_TYPE_cmp function of the OpenSSL component in OpenScape Voice, as documented in CVE-2015-0286. No other Unify product is affected by this vulnerability.

This advisory lists the affected versions of OpenScape Voice and associated recommended actions.
It also provides a note regarding other OpenSSL vulnerabilities that were disclosed between January and July 2015.

Vulnerability Details

The function ASN1_TYPE_cmp of OpenSSL will crash with an invalid read if an attempt is made to compare ASN.1 boolean types. ASN1_TYPE_cmp is used to check certificate signature algorithm consistency. The MTLS-SIP interface of OpenScape Voice (default port: 5161/tcp) may therefore crash if a TLS client sends a specially crafted X.509v3 certificate during the MTLS handshake with OpenScape Voice. This could result in Denial of Service for the MTLS-SIP interface for legitimate clients: SIP Gateways, Session Border Controllers, VoIP-aware Firewalls, or (in OpenScape V8 only) SIP subscribers where MTLS is configured.

Mitre has assigned CVE-2015-0286 to this issue in OpenSSL. Further information is available in the OpenSSL Security Advisory [19 Mar 2015].

CVSSv3 scores for OpenScape Voice:

- Base Score: 5.3 (medium)
- Temporal Score 4.8 (medium)
- CVSS v3 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C)

Additional note about OpenSSL vulnerabilities:
Further vulnerabilities were disclosed for OpenSSL in the time frame January - July 2015.
Unify products are either not affected by these vulnerabilities, or with low risk only; the associated corrections in the OpenSSL component were or are being included accordingly as part of the regular maintenance releases for any Unify product that includes OpenSSL.
This applies to the vulnerabilities listed in the following OpenSSL security advisories: [08 Jan 2015] , [19 Mar 2015], [11 Jun 2015], [9 Jul 2015].
The impact of the latest OpenSSL vulnerabilities ([3 Dec 2015]) to Unify products is described in the Security Advisory OBSO-1512-02.

Affected Products

- **OpenScape Voice V7 R1.42.0** - only if Image V7 R1.42.0_07 (MOP Q3068 - SLES11 SP3 Set3) is installed.
  Earlier releases of V7 are not affected.
- **OpenScape Voice V8 R1.37.x, V8 R1.38.x, V8 R1.39.x**.
  Earlier releases of V8 (up to and including V8 R0.34.4) are not affected.

Recommended Actions

Fix Releases:
Specific upgrade activities are only required if the installed version of OpenScape Voice is among the versions listed above.

- For OpenScape Voice V7: **upgrade to V7 R1.43.1** (release date: 2015-05-13) or any later version
- For OpenScape Voice V8: **upgrade to V8 R1.43.1** (release date: 2015-11-13) or any later version

Mitigation Measures:
The following settings are recommended as general best-practice security hardening in the customer's network - regardless if a fix for this particular issue in the affected Unify product(s) is installed or not.

- Limit the access to the MTLS port of OpenScape Voice (default: **5161/tcp**) from trusted systems only (Gateways, Session Border Controllers etc, where SIP trunks via MTLS are configured).
- Remote MTLS subscribers (OpenScape Voice V8, not available in V7):
  If remote MTLS subscribers are configured and direct access to OpenScape Voice is granted from the Internet: limit the access to known subscriber IP addresses only.
  Note that the general accessibility of OpenScape Voice from the Internet is strongly discouraged. The preferred solution is to install a Session Border Controller or VoIP-aware Firewall in the DMZ. OpenScape Session Border Controller (all versions) is not affected by this vulnerability.

References

- Unify: Security Advisories related with OpenSSL vulnerabilities in 2015:
  - OBSO-1512-01 (this advisory)
  - OBSO-1512-02 (OpenSSL vulnerabilities, Dec. 2015)
- NIST/NVD vulnerability entry: CVE-2015-0286
- OpenSSL Software Foundation: OpenSSL Security Advisory [19 Mar 2015]
- FIRST: Common Vulnerability Scoring System (CVSS), V3

Revision History

2015-12-23: Initial release

Advisory ID: OBSO-1512-01 (a=106), 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