Security Advisory Report - OBSO-1512-02

Multiple Unify Products - TLS Denial of Service Vulnerability in OpenSSL Certificate Verification (CVE-2015-3194)

Creation Date: 2015-12-03 23:51:17
Last Update: 2018-03-27 18:32:21

Summary

The OpenSSL component as included in various Unify products contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition in a TLS client or server implementation.

The risk is rated **medium**.

The issue is caused by a NULL pointer dereference in the function rsa_pss_decode of the OpenSSL component, as documented in CVE-2015-3194 and in the OpenSSL Security Advisory [3 Dec 2015].

This advisory lists the affected versions of Unify products and associated recommended actions.
It also provides a note regarding other OpenSSL vulnerabilities that were disclosed in 2015.

Details

The signature verification routines of OpenSSL will crash with a NULL pointer dereference if presented with an ASN.1 signature using the RSA PSS algorithm and absent mask generation function parameter. These routines are used by Unify products to verify X.509v3 certificate signature algorithms during a TLS handshake between a TLS client and TLS server. Therefore, the vulnerability impacts Unify products in the following cases:

1. Any OpenSSL-based **TLS server (SIP or HFA)** in a Unify product where client authentication is enabled, as in MTLS-SIP or MTLS-HFA connections.
2. Any OpenSSL-based **TLS client (SIP or HFA)** in a Unify product where TLS server certificate verification is enabled (which is a recommended configuration).
3. Any OpenSSL-based **TLS client (**in other connection types such as **https or LDAPS)** in a Unify product where TLS server certificate verification is enabled (which is a recommended configuration).

Mitre has assigned **CVE-2015-3194** to this issue in OpenSSL. Further information is available in the OpenSSL Security Advisory [3 Dec 2015].

CVSSv3 scores for Unify Products:

- Base Score: 5.3 (medium)
- Temporal Score 4.9 (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:W/RC:C)

Additional note about OpenSSL vulnerabilities:
Further vulnerabilities were disclosed in the OpenSSL Security Advisory [3 Dec 2015] as follows: CVE-2015-3193, CVE-2015-3195, CVE-2015-3196, CVE-2015-1794. Unify products are not affected by these vulnerabilities.
The impact of earlier OpenSSL vulnerabilities (disclosed in the time frame January - July 2015) to Unify products is described in the Security Advisory OBSO-1512-01.

Affected Products

Products confirmed as vulnerable:

- OpenScape Voice V8 R1, OpenScape Branch V8 R1, OpenScape SBC V8 R1
- OpenScape 4000 V7 R2 (HG Gateways, Assistant, and Softgate (*); CSTA is not affected)
- OpenScape 4000 Manager V7 R2 (versions before V7 R2 are not affected)
- OpenStage / OpenScape Desk Phone IP SIP: V3 R3.32.0 and later versions
- OpenStage / OpenScape Desk Phone IP HFA: V3 R0.28.0 and later versions
- OpenScape Contact Center Agile/Enterprise V8 R2 and V9 (**)

(*) Softgate was previously listed as not vulnerable, which is correct in default installations. However, installations where MTLS-SIP is enabled for subscriber interfaces are affected.
(**) Affected with low risk only.

Products confirmed as not vulnerable:

- OpenScape Voice V7 R1, OpenScape Branch V7 R1, OpenScape SBC V7 R1
- OpenScape Voice V9, OpenScape Branch V9, OpenScape SBC V9
- OpenScape 4000 V7 R1 and HiPath 4000 V6 R2
- OpenScape 4000 V7 R2: CSTA
- OpenScape 4000 Manager V7 R1 and HiPath 4000 Manager V6 R2
- OpenStage / OpenScape Desk Phone IP SIP: all versions before V3 R3.32.0
- OpenStage / OpenScape Desk Phone IP HFA: all versions before V3 R0.28.0
- All products where a vulnerable version of OpenSSL is either not included or not used for certificate verification, such as:
    - OpenScape UC Application - all servers, clients, apps
    - OpenScape Common Management Portal, Deployment Service, Fault Management, Accounting Management
    - OpenScape Voice Trace Manager
    - OpenScape Alarm Response (OScAR) Eco and Pro
    - OpenScape Office
    - OpenStage Xpert
    - OpenScape Xpressions
    - OpenScape Contact Center Call Director SIP Service (CDSS)
    - OpenScape Desk Phone CP 200/400/600

Recommended Actions

Fix Releases:

- OpenScape Branch and OpenScape SBC: Update to V8 R1.6.0 (INF-16-000117/INF-16-000118, release date: 2016-02-04) or any later version (Note: V8 R1.7.0 or later is recommended, see OBSO-1602-02)
- OpenScape 4000 Manager V7 R2: Update to V7 R2.20.1 (HF004391, release date: 2016-03-07) or any later version
- OpenScape Voice V8 R1: Install Server Image V8 R1.44.0_04 (V8.00.01.ALL.08_PS0044, INF-16-000123, release date: 2016-03-23) or any later version
- OpenScape 4000 Assistant V7 R2: Update to V7 R2.20.2 (HF004428, release date: 2016-04-04) or any later version
- OpenStage and OpenScape Desk Phone IP (SIP): Update to V3 R4.8.0 (release date: 2016-05-02) or any later version
- OpenScape Contact Center Agile/Enterprise V8 R2: Update to V8 R2.15.103 (release date: 2016-06-06) or any later version
- **OpenScape Contact Center Agile/Enterprise V9 R1 Update to V9 R1.2.0 (release date: 2017-10-20) or any later version**
- **OpenScape Contact Center Agile/Enterprise V9 R2 Update to V9 R2.0.1 (release date: 2018-01-16) or any later version**
- OpenScape 4000 Softgate V7 R2: Update to V7 R2.23.4 (LW Hotfix 4 in HF004489, release date: 2016-07-26) or any later version
- OpenStage / OpenScape Desk Phone IP HFA: Update to V3 R0.36.0 (INF-17-000009, release date: 2016-10-04) 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.

Regarding case #1 (as listed in the vulnerability details):

- Limit the access to the MTLS port of OpenScape Voice, Branch, SBC or OpenScape 4000 (Softgate and HG Gateways) from trusted systems only (Gateways, Session Border Controllers etc, where SIP or HFA trunks via MTLS are configured).
- Remote MTLS subscribers (SIP or HFA):
  If remote MTLS subscribers are configured and direct access to OpenScape Voice, Branch, SBC or OpenScape 4000 (Softgate and HG Gateways) is granted from the Internet: limit the access to known subscriber IP addresses only.

Regarding case #2 (as listed in the vulnerability details):

- OpenScape Voice, Branch, SBC, OpenScape 4000: the same measures as described in #1 are valid to protect from potential attacks when these products initiate a TLS handshake as (M)TLS-SIP or (M)TLS-HFA clients.
- OpenStage / OpenScape Desk Phone IP phones (SIP/HFA): Ensure proper configuration of (M)TLS-SIP or (M)TLS-HFA server addresses. Apply suitable measures in the customer

network to prevent potential attackers from impersonating legitimate TLS (SIP/HFA) servers or inserting specially crafted X.509 certificates in the TLS handshake between a phone an the legitimate TLS server.

Regarding case #3 (as listed in the vulnerability details):

- OpenStage / OpenScape Desk Phone IP phones: Ensure proper configuration of LDAPS server and HTTPS server (e.g. for Software Download) addresses. Apply suitable measures in the customer network to prevent potential attackers from impersonating legitimate LDAPS or HTTPS servers or inserting specially crafted X.509 certificates in the TLS handshake between a phone an the legitimate server.

References

- Unify: Security Advisories related with OpenSSL vulnerabilities in 2015:
  - OBSO-1512-01 (OpenSSL vulnerabilities, January - July 2015)
  - OBSO-1512-02 (this advisory)
- NIST/NVD vulnerability entry: CVE-2015-3194
- OpenSSL Software Foundation: OpenSSL Security Advisory [3 Dec 2015]
- FIRST: Common Vulnerability Scoring System (CVSS), V3

Advisory: OBSO-1512-02, 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