Security Advisory Report - OBSO-1408-02

OpenScape Deployment Service - Hardening of the TLS-based Workpoint Interface

Creation Date: 2014-08-22
Last Update: 2015-01-31

Summary

As part of the continuous security improvements, OpenScape Deployment Service V7 R2.4.1 and later have removed the support of various options in its default configuration of the TLS (Transport Layer Security) Protocol, where known weaknesses exist.

As a result, older (post EOL) devices such as OpenStage SIP V2 or OpenStage HFA V2 are no longer supported by default.

Update 2015-01-31: Changes in the default configuration starting with OpenScape Deployment Service V7 R2.7.0/V7 R2.7.1

Risk level: none - this advisory is released for information purposes only.

Vulnerability Details

Unify recommends to update any installation of OpenScape Deployment Service (DLS) to V7 R2.4.1 or later to benefit from improved default security hardening of the TLS-based interface to all managed devices (Phones, Clients, Gateways).
The hardening measures in DLS V7 R2.4.1 include:

- CVE-2009-3555 - Disallow TLS insecure renegotiation
- CVE-2011-1473 - Disallow TLS client-initiated renegotiation
- CVE-2011-3389 - Protect against a fast block-wise chosen-plaintext attack (known as "BEAST" attack)

As a result of this update, older (post EOL) devices such as OpenStage SIP V2 or OpenStage HFA V2 may no longer be manageable via DLS.

Therefore, affected OpenStage phones should be updated to the latest version of OpenStage HFA V3 R0 or SIP V3 R3, respectively, before the update of the DLS can take place.
In cases where the management of phone versions V2 (or older) is still required, an appropriate workaround is described in chapter 4.2.8 of the latest DLS Release Notes.

Update 2015-01-31: Starting with DLS V7 R2.7.0/V7 R2.7.1 (release date: 2015-01-23) the protection against CVE-2011-3389 ("BEAST" attack) has been disabled in the default configuration. Based on an internal security review Unify concludes that the residual risk for "BEAST" attacks against TLS connections of DLS is negligible.
This allows connectivity to older devices as well as the use of the jHPT Service Tool installed directly on the DLS server without additional configuration steps.

Affected Products

- OpenScape Deployment Service V7 R2
- OpenStage HFA before V3
- OpenStage SIP before V3
- jHPT Service Tool

Recommended Actions

See the section "Vulnerability Details" above.

References

Release Notes:

- OpenScape Deployment Service V7 R2.4.1, version 1.1 (2014-08-21)
  chapter 4.2.8 described the workaround to support post EOL OpenStage phone versions
- OpenScape Deployment Service V7 R2.7.0/V7 R2.7.1, version 1.1 (2015-01-28)
  chapter 4.2.8 has been removed as no longer relevant

Revision History

2014-08-22: Initial release
2015-01-31: Update 01:

- Changes in the default configuration starting with OpenScape Deployment Service V7 R2.7.0 and V7 R2.7.1

Advisory ID: OBSO-1408-02 (a=91), 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