Security Advisory Report - OBSO-1511-02

Non-unique X.509 certificates in OpenStage / OpenScape Desk Phone IP (CVE-2015-8251)

Creation Date: 2015-11-30
Last Update: 2015-11-30

Summary

On Nov 25, 2015 a research was published that addresses the use of non-unique X.509 certificates and SSH host keys by embedded devices of multiple vendors. Attackers may misuse known keys to conduct man-in-the-middle attacks or decrypt the communication between a legitimate user and a device.
The research covers more than 4000 embedded devices of over 70 different vendors (including OpenStage VoIP phones by Unify) and identified more than 3 million vulnerable devices on the Internet (including 404 OpenStage devices).
The issue is tracked globally by the CERT Coordination Center (CERT/CC) as VU#566724.

This advisory summarizes the impact for Unify VoIP phones (OpenStage and Desk Phone IP) and provides recommendations how to solve this vulnerability by appropriate configuration of individual keys.
Unify also documents the currently used default keys to emphasize their insignificance with regard to trusted connections between administrators and the device (see Appendix OBSO-1511-02-A).
Updates for the phone software are not planned.

Mitre has assigned the ID CVE-2015-8251 to address the issue for Unify VoIP phones.
The risk is rated as **medium** for insecurely configured phones.

Vulnerability Details

Embedded devices typically include a web based management interface (https) for standard administrative tasks and potentially also a Secure Shell interface (ssh) for expert-level/emergency tasks (command line interface).
Devices should be configured with unique and trusted keys (i.e., a X.509 certificate for https and a host key for ssh); this enables legitimate users to authenticate the device whenever it is accessed from remote.
In cases where non-unique (or otherwise compromised or untrusted) keys are used by the device, attackers may potentially impersonate the device and conduct man-in-the-middle attacks or decrypt the communication between a legitimate user (administrator) and the device.

For more details please refer to CERT/CC Vulnerability Note (VU#566724) and the research publication by Stefan Viehböck (SEC Consult): House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide

Impact to Unify VoIP Phones:

1. Non-Unique SSH Host Keys:
This issue does not apply to Unify VoIP phones, as the key is uniquely created by every device during first startup, including various entropy sources for the random number generation. Furthermore, the following measures prevent from potential malicious use of the ssh interface:

- ssh/port 22 is disabled by default and is only used as a last resort for special troubleshooting tasks; any administrative tasks are available through the standard administration interfaces: Workpoint Interface (WPI) to provisioning tools such as the OpenScape Deployment Service (DLS), and the phone's web based management interface (https/443)
- Enabling ssh/port 22 requires to define a password for one-time use with the intended ssh logon session and to set limits (in minutes) for both:
  - the time until access to ssh is automatically disabled again (thus no access possible anymore)
  - the time until the administrator's ssh session (if established) is automatically logged out
- ssh sessions are executed in the context of a low-privileged account on the Linux platform of the device; only access to the resources relevant for troubleshooting is granted
- The Linux platform and file system is pre-hardened to prevent the ssh session users from raising their privileges to superuser (root) level.

2. Non-Unique X.509 Certificates Used For HTTPS (Web Based Management):
Unify VoIP Phones are delivered with a hard-coded default X.509 certificate that is identical for any phone software released within a given timeframe.
In cases where this hard-coded default certificate remains configured for https connections, a user's (administrator's) browser is unable to authenticate the phone's web server. Attackers who are able to intercept the connection between the browser and the phone may therefore impersonate the web server and conduct man-in-the-middle attacks or decrypt the communication (thus virtually downgrading a https connection to http).

Through an Internet-wide scan the research study identified 404 OpenStage phones open to the Internet where this configuration applies. This small number provides us with confidence that most customers have conducted suitable hardening measures as suggested in the Security Checklist of OpenStage / OpenScape Desk Phone IP. Owners of vulnerable phones should consider the measures listed in the section "Recommended Actions".

CVSSv3 scores (in cases where the hard-coded default certificate for https on a Unify VoIP phone is used)**:**

- 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:L/I:N/A:N/E:F/RL:O/RC:C)

Credits:
We would like to thank Stefan Viehböck (SEC Consult) and CERT/CC for the premature notification and the detailed information exchange with Unify.

Affected Products

- OpenStage 60 / OpenScape Desk Phone IP 55G SIP V3
- OpenStage 15/20E/20/40 / OpenScape Desk Phone IP 35G SIP V3
- OpenScape Desk Phone IP 35G Eco SIP V3
- OpenStage 60 / OpenScape Desk Phone IP 55G HFA V3
- OpenStage 15/20E/20/40 / OpenScape Desk Phone IP 35G HFA V3
- OpenScape Desk Phone IP 35G Eco HFA V3

Recommended Actions

The following measures are usually applied to OpenStage and OpenScape Desk Phone IP phones (SIP or HFA) in enterprise environments. For more details and further recommended hardening measures refer to the corresponding Security Checklist (SIP or HFA).

Note that the individual configuration settings are preferably executed via the Workpoint Interface (WPI), where the phones act as a client towards a central provisioning system such as the OpenScape Deployment Service (DLS). The use of a provisioning system significantly facilitates the management of many phones through bulk change capabilities, incl. the provisioning of cutomized X.509 certificates. OpenScape DLS also features a PKI connector that manages the complete certificate lifecycle for all phones in an enterprise environment where a PKI (Public Key Infrastructure) is in place.

In the context of the issues described in this advisory, the following measures are generally recommended for secure operation of OpenStage and OpenScape Desk Phone IP phones:

- Do not expose the web based management interface (https/443) or any other listener port of the phone to the Internet
- Deactivate the web based management (WBM), if not needed; use the OpenScape Deployment Service (DLS) or an alternate central provisioning service instead
- If the WBM is required:
  - Configure a password policy and set appropriately strong passwords
  - Import and activate a phone-individual SSL/TLS certificate for the WBM's https web server
- When (temporarily) activating the Secure Shell interface for troubleshooting purposes, select a strong one-time password for access and set a short time limit (to automatically disable access after the specified time)

For phones used in an enterprise network:

- Establish best-practice security measures for your VoIP environment, esp. ensure that VoIP devices are operated and managed in a separate VLAN

In cases where phones need to be managed remotely over the Internet (Service Providers or Home Office/Teleworking scenarios):

- Exclusively use the OpenScape Deployment Service (DLS) or an alternate central provisioning service that supports the Workpoint Interface (WPI) implementation of the phones
- Enable Secure Mode for WPI, where mutually authenticated TLS connections based on individual X.509 certificates on both the DLS (server) and the phone (client) side are established
- Use the SIP-Notify mechanism (for SIP phones only), or a DCMP (DLS Contact-Me Proxy, available for both SIP and HFA) to enable the DLS to contact the phones upon request only.

A comprehensive list of hardening recommendations can be found in the planning guides "OpenScape Desk Phone IP/OpenStage SIP V3, Security Checklist" and "OpenScape Desk Phone IP/OpenStage HFA V3, Security Checklist".

References

External links:

- Publication by SEC Consult: House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide
- CERT/CC Vulnerability Note: VU#566724
- NIST/NVD vulnerability entry for OpenStage / OpenScape Desk Phone IP: CVE-2015-8251
- CWE-321: Use of Hard-coded Cryptographic Key

Unify:

- Appendix OBSO-1511-02-A - Default Phone Certificates for OpenStage and Desk Phone IP - web based management interface (https/443)
- Security Checklist for OpenStage / OpenScape Desk Phone IP (SIP or HFA)

Revision History

2015-11-30: Initial release

Advisory ID: OBSO-1511-02 (a=122), 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

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.