

Security Advisory Report - OBSO-1903-02

OpenScape Desk Phones HFA and SIP CSRF and Privilege Escalation vulnerabilities

Release Date: 2019-04-02 16:06:39

Last Update: 2019-04-02 16:06:39

Summary

The firmware of the Unify OpenScape CP IP phone contains several vulnerabilities, which would allow an attacker to control the device.

The attacker has to be in the same network.

To get a remote shell on the device a concatenation of two vulnerabilities is required.

- 1.) Enabling secure shell via CSRF
- 2.) Secure-Shell Privilege Escalation to Root (only possible with ssh access)
- 3.) Authenticated privilege escalation with File-Upload Path traversal

The vulnerabilities were detected by Fraunhofer and reported to Unify and later to VulnDB

Details

- 1.) Enabling secure shell via CSRF

The web interface offers the possibility to enable a secure shell (ssh access) for administration.

This shell can later be used for a privilege escalation in order to permanently control the device.

One possible way of enabling the access to the secure shell without prior authentication is to exploit the missing protection against CSRF (Cross-Site-Request-Forgery).

- 2.) Secure-Shell Privilege Escalation to Root (only possible with ssh access)

Having access to the limited secure shell, a privilege escalation can be performed in order to gain root access and with it full control over the device. Scanning running processes points out that stunnel being run as root.

- 3.) Authenticated privilege escalation with File-Upload Path traversal

Another way for privilege escalation from admin to root has been found within the Ringtone File-Upload feature.

The feature allows you to specify an arbitrary webserver or ftp-server and the absolute path including the filename where the file can be found.

The path and filename are not checked for path traversal.

Affected Products

OpenScape Desk Phone CP SIP V1 R0.1.0 to CP SIP V1 R5.6.0

Fix version: OpenScape Desk Phone CP SIP V1 R5.14.0

OpenScape Desk Phone CP HFA V1 R0.3.0 to CP HFA V1 R2.10.0

Fix version: OpenScape Desk Phone CP HFA V1 R2.11.0

Recommended Actions

Update to the fix versions:

Fix version: OpenScape Desk Phone CP SIP V1 R5.14.0

Fix version: OpenScape Desk Phone CP HFA V1 R2.11.0

References

Vulnerabilites in RBS VulnDB, needs account.

<https://vulndb.cyberiskanalytics.com/vulnerabilities/195003>

<https://vulndb.cyberiskanalytics.com/vulnerabilities/195004>

<https://vulndb.cyberiskanalytics.com/vulnerabilities/195005>

Advisory: OBSO-1903-02, 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

obs@unify.com

© Unify Software and Solutions GmbH & Co. KG 2018

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.