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: 2019-08-23 17:39:22

Summary

Update:

Heise and Fraunhofer articles:

https://www.heise.de/security/meldung/VoIP-Sicherheitsluecken-Viele-Buero-Telefonanlagen-grundlegend-unsicher-4499202.html

https://www.sit.fraunhofer.de/de/cve/

https://www.sit.fraunhofer.de/fileadmin/dokumente/CVE/Advisory_Unify_OpenScape_CP200.pdf?_=1542890694

Update affected products see below.

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.
The vulnerabilites can only be exploited if an **administrator** is logged in and switches on ssh or reacts to a phishing mail.

Risk Level is considered medium

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

Affected products OpenScape Deskphone CP

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

Affected products OpenScape Deskphone IP and OpenStage

OpenScape Desk Phone IP 35G Eco **(SIP)**
OpenStage 15/20E/20/40 & OpenScape Desk Phone IP 35G (SIP)
OpenStage 60 & OpenScape Desk Phone IP 55G (SIP)

Affected:
All OpenStage SIP V1, OpenStage SIP V2, OpenStage SIP V3R0, OpenStage SIP V3R1, OpenStage SIP V3R3, OpenStage SIP V3R4 and OpenStage SIP V3R5 releases prior to V3R5.13.0

Fix version: OpenStage + OpenScape Deskphone IP SIP Software V3 R5.13.0

OpenScape Desk Phone IP 35G Eco **(HFA)**
OpenStage 15/20E/20/40 & OpenScape Desk Phone IP 35G (HFA)
OpenStage 60 & OpenScape Desk Phone IP 55G (HFA)

Affected:
OpenStage + OpenScape Deskphone IP HFA Software V3R0.23.0 to V3 R0.42.1

Fix version: OpenStage + OpenScape Deskphone IP HFA Software V3 R0.43.0 (Pilot at the moment)

Not affected products:

OpenStage 10 (TDM)
OpenStage 15/20/30/40 (TDM)
OpenStage 60 (TDM)

Recommended Actions

Update to the fix versions mentioned above

References

Vulnerabilites in RBS VulnDB, needs account.

https://vulndb.cyberriskanalytics.com/vulnerabilities/195003

https://vulndb.cyberriskanalytics.com/vulnerabilities/195004

https://vulndb.cyberriskanalytics.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
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com