PUBLIC - FOR EXTERNAL USE: (TLP: WHITE)

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Security Advisory Report - OBSO-2312-01

Multiple vulnerabilities affecting Atos Unify IP Devices

Status:	Update Release
Release Date:	2023-12-11 12:26:43
Last Update:	2023-12-15 15:11:48
Version:	1.1

Summary

Multiple vulnerabilities have been identified as part of external security tests that affect Atos Unify IP devices.
When phones are first deployed, the WPI (Work Point Interface) interface is set to default mode. The WPI interface connects the devices to the DLS (Deployment Service) or DLI (Deployment Service Light). An attacker with local access to the network may gain full administrative access to the phone if the WPI interface is in default mode. Mitigation measures are described in the security checklist for the Unify IP devices. Additional information is provided in the Action section. The security test has identified additional vulnerabilities that are described in the Details section.

Customers are advised to update the systems with the available fix releases.
Where issues need to be mitigated by applying configuration measures, follow the instructions of this security advisory and the information provided within the security checklist of the Unify IP device.

The severity is rated high to medium.

We'd like to thank Pentagrid AG for disclosing the vulnerabilities to us.

Details

Pentagrid has disclosed its research on their security blog including proof-of-concept information on how to exploit the vulnerabilities.[1]

Vuln 1: Missing authentication on the WPI (Work Point Interface) in default mode
A remote attacker can enable the Secure Shell feature on the phone by abusing the unauthenticated WPI interface of the phone. It is possible to set an attacker defined password for the admin user, even if there was a password defined.
The CVSS3.1 base score is 8.8 (high)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Vuln 2: Secure Shell privilege escalation to root
A remote attacker with Secure Shell access as admin user is able to abuse improper file permissions to change system-relevant files. An attacker can escalate privileges in order to gain permanent root access on the phone.
The CVSS3.1 base score is 6.7 (medium)
CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Vuln 3: Writable framebuffer
A remote attacker with Secure Shell access as Linux user admin user is able to write into the framebuffer device. An attacker can change the display of the phone.
The CVSS3.1 base score is 3.4 (low)
CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L

Vuln 4: Secure Shell Privilege escalation to root
A remote attacker with Secure Shell access as admin user is able to abuse SetUID permissions to change system-relevant files. An attacker can escalate privileges in order to gain permanent root access on the phone.
The CVSS3.1 base score is 6.7 (medium)
CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Vuln 5: Phone does not verify TLS certificate of DLS server per default
The phone does not verify the TLS certificate when connecting to the DLS server, with standard settings. This allows man-in-the-middle attackers to spoof a DLS connection. An attacker could also host their own DLS server with an arbitrary certificate.
The CVSS3.1 base score is 4.3 (medium)
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Affected Products

Product statements are related only to supported product versions. Products which have reached End of Support (M44) status are not considered.

Products confirmed affected

Vuln #	Internal reference	Product versions affected	Mitigation
Vuln 1		All software versions (Note 1)	Configuration change (Note 1) / Security Checklist
Vuln 2	DWE-19686 DWEH-5763 DCOA-4670	Atos Unify OpenScape Desk Phones CP SIP V1 before V1 R10.4.1 Atos Unify OpenScape Desk Phones CP HFA V1 before V1 R7.5.0 Atos Unify OpenScape Desk Phones CP SIP & HFA V2 before V2 R0.13.0	available available available

Vuln 3	DWE-19685 DWEH-5764 DCOA-4671	Atos Unify OpenScape Desk Phones CP SIP V1 before V1 R10.4.1 Atos Unify OpenScape Desk Phones CP HFA V1 before V1 R7.5.0 Atos Unify OpenScape Desk Phones CP SIP & HFA V2 before V2 R0.13.0	available available available
Vuln 4	DWE-19684 DWEH-5765 DCOA-4677	Atos Unify OpenScape Desk Phones CP SIP V1 before V1 R10.4.1 Atos Unify OpenScape Desk Phones CP HFA V1 before V1 R7.5.0 Atos Unify OpenScape Desk Phones CP SIP & HFA V2 before V2 R0.13.0	available available available
Vuln 5		All software versions	Configuration change/Security Checklist

Additional Notes

Note 1) The following additional mitigation options are introduced with the fix versions listed below:

- Option to disable WPI to solve the issue
- Option to lock the DLS IP address to harden the connection between DLS and phone

Atos Unify OpenScape Desk Phones CP SIP V1.10.4.3 (available)
Atos Unify OpenScape Desk Phones CP HFA V1.7.5.1 (available)
Atos Unify OpenScape Desk Phones CP SIP & HFA V2 V2R0.13.0 (available)

Vulnerability 1 also affects OpenScape Desk Phone IP and OpenStage phone models that are End of Support.

Note 2) OpenScape Desk Phone software versions related to the following phone models

Software versions	**Phone models**
Atos Unify OpenScape Desk Phones CP SIP V1 Atos Unify OpenScape Desk Phones CP HFA V1	OpenScape Desk Phone CP 100 / 20x / 600E / 600 / 700 / 700X
Atos Unify OpenScape Desk Phones CP SIP V2 Atos Unify OpenScape Desk Phones CP HFA V2	OpenScape Desk Phone CP 110 / 210 / 410 / 710

Recommended Actions

Customers are advised to update the systems with the available fix release and follow the recommendation of the Security Checklist of the respective Unify IP device family.

Additional recommendations:

It is generally recommended to use DLS Secure Mode. If Secure Mode is enabled phones will automatically validate the DLS certificate (and vice versa).

For vulnerability 1: Missing authentication on the WPI (Work Point Interface) in default mode

General risk:
- WPI interface in default mode is not secured against remote attackers with access to the local network
- An attacker with local access to the network may gain full administrative access to the phone

<u>1. For Unify IP devices deployed with Atos Unify OpenScape Voice and Atos Unify OpenScape 4000</u>

a) Best practice recommendation
a1) For new installations
For these phones, please complete the following security instructions:
- Deploy Atos Unify OpenScape phones using Atos Unify OpenScape DLS
- Complete the initial phone configuration in a staging environment using a staging DLS
- Replace the default certificate
- Configure secure mode for communication with the DLS
- Configure the IP address of the production DLS server via DHCP
- Deploy phones to the production environment

a2) For existing installations
- Deploy Atos Unify OpenScape phones using Atos Unify OpenScape DLS
- Replace the default certificate
- Configure secure mode with pin for communication with the DLS
- Configure the IP address of the production DLS server via DHCP

b) Alternative options with increased exposure
b1) Deploy DLS address via DHCP
Exposure of the phone (remaining risk)
- The phone will only respond to the DLS Server ip address configured
- IP addresses may be spoofed or phones could connect to a rogue DHCP server
- Eavesdropping on DLS-WPI communications is possible

b2) DLS Secure Mode (without staging / without pin)
- Replace default DLS certificate
- Configure secure mode no pin for communication with the DLS

Exposure of the phone (remaining risk)
- Initial bootstrap of the phone when contacting DLS may be intercepted

<u>2. For Unify IP devices deployed with Atos Unify OpenScape Business</u>

a) In environments with high-security standards use OpenScape DLS to manage the phones, see the recommendations in point 1.

b) In standard OpenScape Business solutions use OpenScape Business embedded DLI (Deployment Service Integrated)
- Manage the phones using the DLI (Deployment Service Integrated)

- Deploy the DLI address via DHCP
- If DHCP is not used restrict communication with the WPI interface to a configured IP address of the DLI (see Note 1)

Exposure of the phone (remaining risk):
- If the DLI address is configured via DHCP, the phone will only respond to the DLI IP address
- If the DLI address is not configured via DHCP, the IP address of the DLI is not validated
- IP addresses may be spoofed, or phones could connect to a rogue DHCP server
- Eavesdropping on DLS-WPI communications is possible

3. For Unify IP devices that are unmanaged

- Deactivate the WPI interface through local configuration (see Note 1)

Alternative options with increased exposure:
- Deploy a DLS server address via DHCP or configure locally on the phone although a DLS is not used for management.

Exposure of the phone (remaining risk):
- The phone will only respond to the configured DLS Server IP address
- IP addresses may be spoofed, or phones could connect to a rogue DHCP server
- Eavesdropping on DLS-WPI communications is possible

For vulnerability 5: Phone does not verify TLS certificate of DLS server per default
It is generally remommended to use DLS Secure Mode. If Secure Mode is enabled phones will automatically validate the DLS certificate.(and vice versa)
Follow the instructions of the security checklist, deploy customer specific certificates, and set the certificate validation to full.

References

[1] Pentagrid Security Blog
[2] For information about hardening the DLS interface to the Phone (WPI interface) check **section 4.2.3 Harden DLS Interface to the Phone of the OpenScape Desk Phone of the CP100/20X/400/600/600E/700/700X Security Checklist**
[3] For information about the different operating modes of the WPI interface refer to **section 3.14 DLS manual Configuration & Update Service (DLS) of the OpenScape Deployment Service V10 Security Checklist**
[4] For the automated distribution of an IP address for DLS/DLI see **section 2.3.8   Vendor Specific: VLAN Discovery and DLS Address of the OpenScape Desk Phone CP Family SIP Administrator Documentation**. Check How to Use Option #43 "Vendor Specific".
[5] For information on new phone features (Lock DLS address / Disable DLS-WPI) introduced fo OpenScape Desk Phone CP V1 refer to the following product documentation:
OpenScape Desk Phone CP Family HFA, Administrator Documentation, Issue 20, chapter 3.3.8, p.66
OpenScape Desk Phone CP Family SIP, Administrator Documentation, Issue 20, 3.4.11, p. 85

Version Change History

Version	Date	Description
1.0	11.12.2023	- Initial release
1.1	15.12.2023	- OpenScape Desk Phones CP SIP & HFA V2 V2R0.13.0 (available)

Advisory: OBSO-2312-01, status: update release
Security Advisories are released as part of Mitel 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

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.