
PUBLIC - FOR EXTERNAL USE: ([TLP: WHITE](#))

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

Security Advisory Report - OBSO-2404-01

Credentials disclosure vulnerability in Unify OpenScape Desk Phones CP

Status:	Update Release
Release Date:	2024-04-03 12:30:49
Last Update:	2024-04-04 15:13:34
Version:	1.1

Summary

A credentials disclosure vulnerability in the Unify OpenScape Desk Phone CP phones, allows an unauthenticated attacker, with physical access to conduct unauthorized access, potentially leading to the exposure of sensitive information. A successful exploit of this vulnerability could allow an attacker to extract sensitive data.

Although exploiting this vulnerability may disclose sensitive data, we have implemented alternative controls to mitigate any potential risks associated with this issue. As a result, this vulnerability poses no significant risk to the phone's security.

Credit is given to Moritz Abrell of SySS GmbH for highlighting these issues and bringing these to our attention.

Details

CVSS3.1 Base score: 2.4 (low)

[AV:P/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

The following products have been identified as affected:

Product Name	Affected Version(s)	Available Solution(s)
OpenScape Desk Phone CP	CP100, 20x, 400_600_600E_700_700X SIP V1R11.2.0 and earlier	Upgrade to fixed version V1R11.3.0
	CP100, 20x, 400_600_600E_700_700X HFA V1R8.1.0 and earlier	Upgrade to fixed version V1R8.2.0
	CP110, 210, 410, 710 V2R0.13.1 and earlier	Upgrade to fixed version V2R0.14.0

Recommended Actions

Customers with affected product versions are advised to update the systems with the available fixes.

References

- CVE-2024-28065
- CVE-2024-28066

Version Change History

Version	Date	Description
1.0	03.04.2024	- Initial release
1.1	04.04.2024	- Minor corrections on fix version names

Advisory: OBSO-2404-01, 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

© Unify Software and Solutions GmbH & Co. KG 2024

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.