Security Advisory Report - OBSO-2305-03

Multiple vulnerabilities in Atos Unify OpenScape Xpressions (CVE-2023-40265/CVE-2023-40266)

Status:	Update Release
Release Date:	2023-05-22 08:23:17
Last Update:	2024-02-12 18:26:19
Version:	1.1

Summary

Multiple vulnerabilities have been identified in Atos Unify OpenScape Xpressions WebAssistant. The combination of the vulnerabilities allows an authenticated attacker arbitrary code execution on the operating system in the context of the web server user.

The severity is rated high to medium.

Customers are advised to update the systems with the available hotfixes as quickly as possible.

We'd like to thank milCERT AT for disclosing and supporting us to remediate the issues.

Details

The vulnerabilities have been privately disclosed by milCERT AT. There are currently no known public exploits.

Vulnerabilities referenced in this advisory affect the following components of the Atos Unify OpenScape Xpressions:

CVE-number	Internal reference	Component affected	Type of vulnerability	Severity	CVSS3.1 Base Score
CVE-2023-40265	UCBE-32133	OpenScape Xpressions WebAssistant	Authenticated remote code execution via file-upload in WebAssistant	High	7.2
CVE-2023-40266	UCBE-32350	OpenScape Xpressions WebAssistant	Path traversal in WebAssistant	Medium	6.5

Affected Products

Product statements are related to product versions before End of Support (M44) is reached

Products confirmed affected

Atos Unify OpenScape Xpressions V7 before V7R1 FR5 HF42 P911 (WebAssistant-811FR5-20937 hotfix) (available)

Recommended Actions

Customers are advised to update the systems with the available fixes as quickly as possible.

Workarounds:

- Do not publicly expose the OpenScape Xpressions web assistant interface

References

Version Change History

Version	Date	Description
1.0	22.05.2023	- Initilal release

Version	Date	Description
1.1	12.02.2024	- Added CVE-numbers

Advisory: OBSO-2305-03, 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.