

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

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

Security Advisory Report - OBSO-2306-01

Multiple vulnerabilities affecting Atos Unify OpenScape 4000 Assistant and Atos Unify OpenScape 4000 Manager

Status: General Release
Release Date: 2023-06-14 14:36:00
Last Update: 2023-06-14 14:36:00
Version: 1.0

Summary

Multiple vulnerabilities have been identified in Atos Unify OpenScape 4000 Assistant and Atos Unify OpenScape 4000 Manager. The vulnerability with the highest severity may allow an authenticated attacker to elevate privileges and run arbitrary code in the context of the root user.

The overall severity is rated high.

Customers are advised to update the systems with the available fixes as quickly as possible. If systems cannot be updated apply the available workarounds.

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

Details

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

Additional Notes:

Vulnerabilities referenced in this advisory affect the following components of the OpenScape 4000 Assistant and OpenScape 4000 Manager:

Internal reference	Component affected	Type of vulnerability	Severity	CVSS Base Score	CVSS Env. Score
OSFOURK-24034	Atos Unify OpenScape 4000 Manager AScm	Privilege escalation may allow an authenticated attacker to run arbitrary code	High	8.8	8.2
OSFOURK-24039	Atos Unify OpenScape 4000 Assistant ASHbr Atos Unify OpenScape 4000 Manager ASHbr	Authenticated Command Injection with an unspecified impact	High	7.2	6.7
OSFOURK-23722	Atos Unify OpenScape 4000 Assistant ASHbr Atos Unify OpenScape 4000 Manager ASHbr	Exposure of sensitive information may allow lateral movement to the backup system	Medium	6.7	6.2

Affected Products

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

Products confirmed affected

Internal reference	Sev.	Product Versions Affected
OSFOURK-24034	H	Atos Unify OpenScape 4000 Manager V10 R1 before V10 R1.42.1 Atos Unify OpenScape 4000 Manager V10 R0 (Note 1)
OSFOURK-24039	H	Atos Unify OpenScape 4000 Assistant V10 R1 before V10 R1.42.1 Atos Unify OpenScape 4000 Assistant V10 R0 (Note 1) Atos Unify OpenScape 4000 Manager V10 R1 before V10 R1.42.1 Atos Unify OpenScape 4000 Manager V10 R0 (Note 1)
OSFOURK-23722	M	Atos Unify OpenScape 4000 Assistant V10 R1 before V10 R1.34.7 Atos Unify OpenScape 4000 Assistant V10 R1.42.0 Atos Unify OpenScape 4000 Assistant V10 R0 (Note 1) Atos Unify OpenScape 4000 Manager V10 R1 before V10 R1.34.7 Atos Unify OpenScape 4000 Manager V10 R1.42.0 Atos Unify OpenScape 4000 Manager V10 R0 (Note 1)

Products confirmed not affected

Internal reference	Sev.	Product Versions Affected
OSFOURK-24034	H	Atos Unify OpenScape 4000 Manager V10 R1.42.1 and higher Atos Unify OpenScape 4000 Assistant V10
OSFOURK-24039	H	Atos Unify OpenScape 4000 Assistant V10 R1.42.1 and higher Atos Unify OpenScape 4000 Manager V10 R1.42.1 and higher
OSFOURK-23722	M	Atos Unify OpenScape 4000 Assistant V10 R1.34.7 and higher hotfixes Atos Unify OpenScape 4000 Assistant V10 R1.42.1 and higher Atos Unify OpenScape 4000 Manager V10 R1.34.7 and higher hotfixes Atos Unify OpenScape 4000 Manager V10 R1.42.1 and higher

Additional Notes

Note 1: No fixes are planned for Atos Unify OpenScape 4000 Assistant V10 R0 and Atos Unify OpenScape 4000 Manager V10 R0

Recommended Actions

Customers are advised to update the systems with the available Hotfixes or the Fix Release as quickly as possible.

Available Fixes:

- Atos Unify OpenScape 4000 Assistant Hotfix V10 R1.42.1 (available) (Note 2)
- Atos Unify OpenScape 4000 Manager Hotfix V10 R1.42.1 (available) (Note 2)
- Atos Unify OpenScape 4000 Assistant Hotfix V10 R1.34.7 (available) (Note 2)
- Atos Unify OpenScape 4000 Manager Hotfix V10 R1.34.7 (available) (Note 2)

Workarounds:

- Do not publicly expose OpenScape 4000 administrative interfaces
- Restrict administrative access to the OpenScape 4000 Assistant and OpenScape 4000 Manager by restricting access to known ip networks/host ip addresses that require access
- Restrict access to the OpenScape 4000 Assistant / Manager administration port within external firewall
- Provide access to the OpenScape 4000 Assistant / Manager administration port through change management procedures when required

Additional Notes:

Note 2: Can be activated without any telephony downtime on Simplex or Duplex systems

References

Version Change History

Version	Date	Description
1.0	14.06.2023	- Initial release

Advisory: OBSO-2306-01, status: general release

Security Advisories are released as part of Atos 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 2023

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.