Security Advisory Report - OBSO-2211-02

Command injection vulnerability in Atos Unify OpenScape 4000 Assistant and Atos Unify OpenScape 4000 Manager (CVE-2022-46404)

Status:	Update Release
Release Date:	2022-11-28 11:34:32
Last Update:	2023-06-19 07:47:17
Version:	1.1

Summary

PUBLIC - FOR EXTERNAL USE (TLP: WHITE)

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

A command injection vulnerability has been identified in Atos Unify OpenScape 4000 Assistant and Atos Unify OpenScape 4000 Manager that may allow an unauthenticated attacker to upload arbitrary files and get administrative access to the system.

The severity is rated critical.

Customers are advised to update the systems with the available hotfixes 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

CVSS3.1 Base score: 9.8 (critical)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

With workarounds applied as defined in **Actions** below:
CVSS3.1 Environmental score: 8.6 (high)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C/CR:H/IR:H/AR:H/MAV:A/MAC:L/MPR:N/MS:U/MC:H/MI:H/MA:H

Affected Products

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

Products confirmed affected

Atos Unify OpenScape 4000 Assistant V8 and V10 before V8 R2.22.18 / V10 R0.28.13 / V10 R1.34.4
Atos Unify OpenScape 4000 Manager V8 and before V10 V8 R2.22.18 / V10 R0.28.13 / V10 R1.34.4

Recommended Actions

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

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

References

Version Change History

Version	Date	Description
1.0	28.11.2022	- Initial release
1.1	19.06.2023	- Added CVE-number

Advisory: OBSO-2211-02, status: update 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

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