Security Advisory Report - OBSO-2303-01

Command injection vulnerabilities in the Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager (CVE-2023- 29473/CVE-2023- 29474/CVE-2023- 29475)

Status:	Update Release
Release Date:	2023-03-20 08:06:27
Last Update:	2023-06-19 07:44:10
Version:	1.3

Summary

3 command injection vulnerabilities have been identified in the Atos Unify OpenScape 4000 Platform and the Atos Unify OpenScape 4000 Manager Platform. The vulnerabilities may allow an unauthenticated attacker to run arbitrary commands on the platform operating system 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 or apply the proposed configuration change.

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.

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 the configuration change applied as defined in **Actions** below:

CVSS3.1 Environmental score: 7.9 (high)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/MAV:A/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H
Based on the following assumptions
- no known public exploits

- issue is mitigated through a configuration change
- interface can be disabled and is usually not exposed to the internet

Additional Notes:

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

Internal reference	CVE	Component affected	Type of vulnerability	Severity	CVSS3.1 Base Score
OSFOURK-23710	CVE-2023-29473	Atos Unify OpenScape 4000 Platform webservice	Unauthenticated command injection	Critcal	9.8
OSFOURK-23552 OSFOURK-23543	CVE-2023-29474 CVE-2023-29475	Atos Unify OpenScape 4000 Platform inventory	Unauthenticated command injection	Critcal	9.8

Affected Products

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

Products confirmed affected

Atos Unify OpenScape 4000 Platform and OpenScape 4000 Manager Platform V10 R1 before V10 R1.34.4

Products confirmed not affected

Atos Unify OpenScape 4000 Platform V10 R0
Atos Unify OpenScape 4000 Platform V8
Atos Unify OpenScape 4000 Manager V10 R0 or older

Recommended Actions

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

implement the proposed configuration change.

Available Fixes:
Atos Unify OpenScape 4000 Platform Hotfix V10 R1.34.4 (see notes (1)and (2))
or
Atos Unify OpenScape 4000 FixRelease V10 R1.42.0 (planned for 31.3.2023)

Mitigation by applying a configuration change for OpenScape 4000 Assistant (3):

As recommended in the OpenScape 4000 V10R1 and Affiliated Products Security Checklist, chapter 7.8.1:

Activate in OpenScape 4000 Assistant GUI under
DE: Zugangsverwaltung -> Sicherheitsmoduskonfiguration -> Anwendungszugriff
EN: Access Management -> Security Mode Configuration -> Application Access
the mode
DE: „Eingeschränkter Zugriff auf das Portal und die SSH der Plattform und der CSTA“
EN: „Restricted access to Platform Portal and SSH of Platform and CSTA”

Additional Notes:
(1) Same Platform Hotfix to be used for OpenScape 4000 **and** OpenScape 4000 Manager
(2) Can be activated without any telephony downtime on Simplex or Duplex systems
(3) Configuration change is not available for OpenScape 4000 Manager

References

Version Change History

Version	Date	Description
1.0	20.03.2023	- Initial release
1.1	24.03.2023	- Added additional notes on affected components
1.2	16.06.2023	- Added CVE-Numbers
1.3	19.06.2023	- Updated title with CVE numbers

Advisory: OBSO-2303-01, 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