PUBLIC - FOR EXTERNAL USE: (TLP: WHITE)

Security Advisory Report - OBSO-2303-02

Command injection vulnerability in Atos Unify OpenScape SBC, Atos Unify OpenScape Branch and Atos Unify OpenScape BCF

Status:	Update Release
Release Date:	2023-03-28 06:26:52
Last Update:	2023-05-08 22:27:10
Version:	1.2

Summary

A command injection vulnerability has been identified for Atos Unify OpenScape SBC, Atos Unify OpenScape Branch and Atos Unify OpenScape BCF. The vulnerability may allow an authenticated attacker with network access to the admin interface and admin privileges to compromise the confidentiality and integrity and availability of the system.

The severity of the vulnerability is rated high to medium.

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

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.

CVSS3.1 Base score: 7.2 (high)
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS3.1 Environmental score: 6.3 (medium)
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:L/IR:L/AR:H/MAV:A/MAC:L/MPR:H/MUI:N/MS:U/MC:H/MI:H/MA:H
Based on the following assumptions
- no known public exploits
- interface is usually not exposed to the internet

Affected Products

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

Products confirmed affected

Atos Unify OpenScape SBC V10 before version V10R3.2.0 (available) (Note 1)
Atos Unify OpenScape Branch V10 before version V10R3.1.2 (available)
Atos Unify OpenScape BCF V10 before version V10R10.7.0 (available as eeQA-FT)

Additional Notes

Note 1: Original fix version V10R3.1.3 has been declared obsolete proactively due to a SSP specific functional issue reported from the customer field.

Recommended Actions

Workarounds:

- Disable low-privileged accounts (e.g guest account) or disable ssh access for the accounts
- Make sure root account is not accessible via ssh
- Restrict external ssh access to a single account
- Do not publicly expose the admin interface of the affected systems
- Implement best practice configuration for **OpenScape Session Border Controller** published in **OBSO-2110-01 Atos Unify Product Security Configuration Note**
- Restrict access to the SBC admin interfaces through a firewall to known IP-addresses to reduce the exposure

Mitigations:

- Apply the patches that are available for the respective product

References

- **OBSO-2110-01 Atos Unify Product Security Configuration Note**

Version Change History

Version	Date	Description
1.0	28.03.2023	- Initial version
1.1	29.03.2023	- Issue is fixed in Atos Unify OpenScape BCF V10R10.7.0 (available as eeQA-FT)
1.2	08.05.2023	- OpenScape SBC V10R3.1.3 has been declared obsolete, new fix version is OpenScape SBC V10R3.2.0

Advisory: OBSO-2303-02, 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