Security Advisory Report - OBSO-2310-01

Argument injection vulnerability in Atos Unify OpenScape SBC, Atos Unify OpenScape Branch and Atos Unify OpenScape BCF (CVE-2023-6269)

Status:	Update Release
Release Date:	2023-10-04 15:21:55
Last Update:	2023-12-01 16:22:45
Version:	1.2

Summary

An argument injection vulnerability has been identified for Atos Unify OpenScape SBC, Atos Unify OpenScape Branch and Atos Unify OpenScape BCF. Insufficient input validation in the web interface may allow an unauthenticated attacker to bypass the administrative web interface to execute arbitrary code.

The severity of the vulnerabilities is rated critical.

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

We'd like to thank Armin Weihbold and the SEC Consult Vulnerability Lab for disclosing and supporting us to remediate the issues.

Details

1) Argument injection leading to unauthenticated RCE and auth bypass (CVE-2023-6269)
The administrative web interface insufficiently escapes supplied login credentials before passing them to a user management application, leading to an unauthenticated attacker being able to gain root access to the appliance
via SSH.

Another possibility to exploit this vulnerability is to append a special argument during logon to completely bypass the authentication of the web interface. A previously unauthenticated attacker can logon as administrator without any known credentials.

CVSS3.1 Base score: 10 (critical)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

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 V10 R3.4.0 (available)

Atos Unify OpenScape Branch V10 before V10 R3.4.0 (available)

Atos Unify OpenScape BCF V10 before V10R10.12.00 (available) and 10R11.05.02 (planned for 31.10.2023)

Additional Notes:
Atos Unify OpenScape BCF is maintained by Atos Public Safety. A statement regarding the impact of the vulnerability has been included in agreement with Atos Public Safety.

Recommended Actions

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

The following workarounds may serve as additional hardening measures. Nonetheless implementing the fix release is required to remediate the vulnerability.

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

References

Version Change History

Version	Date	Description
1.0	04.10.2023	- Initial release
1.1	09.10.2023	- Added Atos Unify OpenScape BCF

Version	Date	Description
1.2	01.12.2023	- Added CVE-number - Updated CVSS-score

Advisory: OBSO-2310-01, 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

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