Security Advisory Report - OBSO-2307-01

Multiple vulnerabilities in Atos Unify OpenScape SBC, Atos Unify OpenScape Branch and Atos Unify OpenScape BCF (CVE-2023-36618/CVE-2023-36619)

Status:	General Release
Release Date:	2023-07-06 16:38:36
Last Update:	2023-07-06 16:38:36
Version:	1.0

Summary

Multiple vulnerabilities have 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 authenticated attacker with low privileged access to the web interface to execute arbitrary code. An unauthenticated attacker may run PHP scripts and cause a denial of service of the system or modify the configuration.

The severity of the vulnerabilities is rated high.

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) Authenticated Remote Code Execution
The API of the administrative web application insufficiently validates the input of authenticated users at the server. This leads to the possibility of executing arbitrary PHP functions (with some defined exceptions) and
subsequently operating system level commands with root privileges. A low-privileged Read-Only role is sufficient to exploit this security issue.

2) Missing Authentication
A number of scripts that are used to administer the appliance can be accessed or executed unauthenticated via the web server. The execution of the scripts may cause a denial of service of the system or change the system configuration.

Additional Notes:

Vulnerabilities referenced in this advisory affect the following components :

Internal reference	CVE	Component affected	Type of vulnerability	Severity	CVSS Base Score
SBC-12679	CVE-2023-36618	Atos Unify OpenScape SBC web interface Atos Unify OpenScape Branch web interface Atos Unify OpenScape BCF web interface	Authenticated remote code execution in web interface	High	8.8
SBC-12680	CVE-2023-36619	Atos Unify OpenScape SBC PHP scripts Atos Unify OpenScape Branch PHP scripts Atos Unify OpenScape BCF PHP scripts	Missing authentication in PHP scripts	High	8.2

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 R3.3.0 (available)

Atos Unify OpenScape Branch V10 before V10 R3.3.0 (available)

Atos Unify OpenScape BCF V10 before V10 R10.10.0 (available)

Recommended Actions

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

If you cannot update immediately, implement the suggested workarounds as they will significantly reduce the exposure.

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	06.07.2023	- Initial release

Advisory: OBSO-2307-01, 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

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