

PUBLIC - FOR EXTERNAL USE: ([TLP: WHITE](#))

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

Security Advisory Report - OBSO-2305-02

Multiple vulnerabilities affecting Atos Unify OpenScape Voice Trace Manager

| | |
|---------------|---------------------|
| Status: | General Release |
| Release Date: | 2023-05-22 08:13:38 |
| Last Update: | 2023-05-22 08:13:38 |
| Version: | 1.0 |

Summary

Multiple vulnerabilities have been identified in Atos Unify OpenScape Voice Trace Manager. The combination of the vulnerabilities may allow an unauthenticated attacker to get full administrative access to the system. User interaction is required for successfully exploiting the vulnerability. Refer to the Details section for additional information.

The severity is rated critical.

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

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.

Additional Notes:

Vulnerabilities referenced in this advisory affect the following components of the OpenScape Trace Manager

| Internal reference | Component affected | Type of vulnerability | Severity | CVSS3.1 Base Score |
|--------------------|---|--|----------|---------------------|
| OSVTM-835 | Atos Unify OpenScape Voice Trace Manager administration | Unauthenticated Stored Cross-Site-Scripting (XSS) via Access Request | Critical | 9.6 |
| OSVTM-836 | Atos Unify OpenScape Voice Trace Manager ftp service | Authenticated Command Injection via ftp | High | 7.2 |
| OSVTM-868 | Atos Unify OpenScape Voice Trace Manager user interface | Authenticated path traversal | High | 7.7 |

Affected Products

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

Products confirmed affected

Atos Unify OpenScape Voice Trace Manager V8 before V8 R0.9.11 (available)

Recommended Actions

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

References

Version Change History

| Version | Date | Description |
|---------|------------|-------------------|
| 1.0 | 22.05.2023 | - Initial release |

Advisory: OBSO-2305-02, 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

© **Unify Software and Solutions GmbH & Co. KG 2023**

Otto-Hahn-Ring 6

D-81739 München

www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.