Security Advisory Report - OBSO-2002-01

OpenScape UC - Multiple vulnerabilities

Release Date: 2020-02-17 15:04:16
Last Update: 2020-02-18 18:14:00

Summary

Multiple vulnerabilities have been identified within OpenScape UC Application that expose the application to various threats.
An attacker with local access privileges to the UC application may be able to gain illegitimate access to conferences.
UC application delivers an **unused application component** that may publicly expose an admin login page. The admin interface is protected against brute force attacks. If successfully exploited the component leaks information on the local file system structure, files and folder names.

The risk level is rated "medium".

Details

Refer to the release notes and the information provided in the security checklist referenced within the **Actions** section below for additional information.

Affected Products

OpenScape UC Application V9 and V10 are affected

- V9 before version V9 R4.31.0
- V10 before version V10 R0.6.0

Recommended Actions

If you are not yet on V9 R4 or V10 upgrade you UC application.

The following patches are provide fixes for the issues.:

- V9 R4.29.0 and V9 R4.31.0
- V10 R0.5.0 and V10 R0.6.0

Refer to the security checklist listed in the **References** section and validate whether you need the conferencing feature described.
If you don't need it, it is recommended to set EnableConferencingRestrictedMode = True.

Note: Security improvements may be included in any release without explicit notification, make sure you continuously apply the latest patches provided.

References

Release notes:

- V9 R4.29.0 (UCBE-21808, UCBE-21809)
- V9 R4.31.0 (UCBE-22311)
- V10 R0.5.0 (UCBE-21808, UCBE-21809)
- V10 R0.6.0 (UCBE-22298)

Note: Release Notes will be updated accordingly

Security Checklist:

- OpenScape UC Application V9 Security Checklist (Issue 14), chapter 5.6
- OpenScape UC Application V10 Security Checklist (Issue 2), chapter 5.6

Advisory: OBSO-2002-01, status: general release
Security Advisories are released as part of 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 2020
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.