



Security Advisory Report - OBSO-1401-05

OpenScape UC Applications - Cross-site Scripting Vulnerability

Creation Date: 2014-01-31
Last Update: 2014-01-31

Summary

The web interface of OpenScape UC Applications (UC App) is vulnerable to a cross-site scripting attack, that allow attackers to redirect other users' UC session requests to a web location outside the domain configured for UC App.

The risk is rated **medium** (CVSS Base Score: 6.1).

Vulnerability Details

The vulnerability is caused by missing input data validation in the single-sign-on function of the web interface of UC App.

Attackers may trick other users to click on specially crafted URLs that - while performing regular authentication at the UC Application - transfer the victim user's session information to an external site.

Affected Products

- OpenScape UC Applications, all versions

Recommended Actions

Upgrade OpenScape UC Applications to V7 R1.2.0 (released: 2013-08-09) or any later version of V7 R1.

Installations, where the access for Web Clients to the UC Application Frontend is protected by appropriate configuration in a WAF (Web Application Firewall) or Reverse Proxy are not affected: disallow any redirection of UC Application web requests to any other domain outside of "https://<your-UC-application-server-domain>".

References

N.A.

Revision History

2014-01-31: Initial release

Advisory ID: OBSO-1401-05 (a=72), 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
obsso@unify.com
© Unify Software and Solutions GmbH & Co. KG 2014
Mies-van-der-Rohe Str. 6, D-80807 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.