



Security Advisory Report - OBSO-1505-03

OpenScape UC Web Client and Desktop Client - Cross-Site Scripting (XSS) Vulnerability

Creation Date: 2015-05-22

Last Update: 2015-05-22

Summary

The Web Client in OpenScape UC Application V7 R2 before V7 R2.1.7 contains an output sanitization error in the instant messaging window. This may enable authenticated attackers to perform cross-site scripting attacks against other legitimate users of the UC Instant Messaging function.

The risk is rated as "medium".

Vulnerability Details

The Web Client contains an output sanitization error (as defined in the Common Weakness Enumeration [CWE-116](#)) when processing html code in the instant messaging window.

Authenticated attackers may be able to send specially crafted html messages to other users that run a vulnerable version of the Web Client or Desktop Client (web embedded). This could lead to cross-site scripting attacks against legitimate users of the UC Instant Messaging function.

Risk level: medium

CVSS Base Score: 4.0, CVSS Temporal Score: 3.1

CVSS v2 Vector (AV:N/AC:L/Au:S/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Affected Products

- OpenScape UC Application V7 R2 before V7 R2.1.7
Both Web Client and Desktop Client (web embedded) are affected

OpenScape UC Application V7 R1 and earlier versions are not affected.

Recommended Actions

Upgrade to OpenScape UC Application V7 R2.1.7 (release date: 2015-04-24) or later to solve this vulnerability.

References

Mitre: Common Weakness Enumeration [CWE-116](#)

Revision History

2015-05-22: Initial release

Advisory ID: OBSO-1505-03 (a=113), 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

obs@unify.com

© Unify Software and Solutions GmbH & Co. KG 2015

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.