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