



Security Advisory Report - OBSO-1501-03

OpenScape Business UC Suite - SQL Injection Vulnerability (CVE-2015-1183)

Creation Date: 2015-01-27

Last Update: 2015-01-27

Summary

OpenScape Business V1 before V1 R3.3.0 contains an SQL injection vulnerability at the web interface for the UC Suite. The risk is rated **high**.

We recommend customers to upgrade to the latest version of OpenScape Business at the earliest opportunity.

Vulnerability Details

OpenScape Business V1 before V1 R3.3.0 contains an SQL injection vulnerability (as defined in the Common Weakness Enumeration [CWE-89](#)) at the web interface for the UC Suite (port https/8802). It may allow remote unauthenticated attackers to modify data, incl. sensitive data such as logon passwords of OpenScape Business mobile users, as well as to download communication data such as log, voice and fax messages.

The vulnerability is relevant only if the **UC Suite** is used (i.e. with an active UC Booster Card or UC Booster Server, or installations of OpenScape Business S).

Standard installations (with **UC Smart** embedded) are not affected.

CVSS scores:

- Base Score: 7.5
- Temporal Score 6.5
- CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:H/RL:OF/RC:C)

Mitre (cve.mitre.org) has assigned the id **CVE-2015-1183** to this issue.

Credits to: George Haddad (Deutsche Telekom AG) for discovery, reporting and the coordinated analysis and disclosure of this vulnerability.

Affected Products

- OpenScape Business X1/X3/X5/X8 V1 with active UC Booster Card or UC Booster Server
- OpenScape Business S V1
- OEM product Octopus F X V1 with active UC Booster Card or UC Booster Server
- OEM product Octopus F X8 S-BS V1

All products are affected in versions before V1 R3.3.0.

Recommended Actions

We recommend customers to **upgrade to V1 R3.3.0 (release date 2015-01-27) or later** at the earliest opportunity.

The following mitigation measures are available:

- Completely deactivate UC Suite access, if not used
- If used: restrict access to the internal network only and apply suitable network security measures to restrict access to legitimate users/devices of the UC Suite
- Disable port-forwarding of https/8802 to the WAN/Internet, until OpenScape Business is upgraded to V1 R3.3.0 or later

References

Mitre:

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1183>
- [CWE-89](#)

Revision History

2015-01-27: Initial release

Advisory ID: OBSO-1501-03 (a=101), 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.