



Security Advisory Report - OBSO-1312-02

OpenScape Voice Trace Manager - Multiple Vulnerabilities in PHP

Creation Date: 2013-12-20

Last Update: 2013-12-20

Summary

OpenScape Voice Trace Manager V7 R0.7.9 was released to address security vulnerabilities in its PHP-based web application.

All vulnerabilities were rated as medium risk for existing installations.

Vulnerability Details

The table below provides an overview of all vulnerabilities relevant to OpenScape Voice Trace Manager (OSV TM) that were solved with V7 R0.5.9.

Vulnerability ID (ref. to cve.mitre.org)	Description	Impact to OSV TM	Risk Level	Vendor Advisory and Details
PHP.net:				
CVE-2013-4248	openssl - TLS Certificate Validation Vulnerability	Remote attackers may spoof TLS connections of OSV TM by specially crafted X.509v3 certificates.	medium	PHP 5.4.18
CVE-2013-4113	XML Parser - Buffer Overflow Vulnerability	Remote attackers may use crafted XML documents to cause a heap-based buffer overflow in the OSV TM application. Successful exploitation may allow execution of arbitrary code on the OSV TM server.	medium	PHP 5.4.18
CVE-2013-2110	quoted_printable_encode - Buffer Overflow Vulnerability	Remote attackers may use crafted input strings to cause a heap-based buffer overflow in the OSV TM application. Successful exploitation may crash the OSV TM application.	medium	PHP 5.4.16

Note: the associated vendor advisories may also include solutions for various other vulnerabilities (identified through different CVE numbers). However, these additional corrections are not relevant in the context of OSV TM and therefore not listed here.

Affected Products

- OpenScape Voice Trace Manager (all versions)

Recommended Actions

Update OpenScape Voice Trace Manager (all versions) to the following version, or higher::

- V7 R0.7.9, release date: 2013-12-18

References

Relevant references to vendor advisories (PHP.net) and to Mitre are given in table in the section "Vendor Advisory and Details".

Revision History

2013-12-20: Initial release

Advisory ID: OBSO-1312-02 (a=66), 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 2013

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.