# Security Advisory Report - OBSO-1501-02

## OpenStage / OpenScape Desk Phone IP - Input Validation Vulnerability via Web Interface (CVE-2014-9563)

Creation Date: 2015-02-26
Last Update: 2015-02-26

## Summary

The web-based management (WBM) of OpenStage / OpenScape Desk Phone IP SIP in V3 before V3 R3.32.0 contains an input validation vulnerability that could allow illegitimate access to the phone's debug interface at the local serial port.

The risk is rated low.

This advisory also lists additional vulnerabilities in OpenStage / OpenScape Desk Phone IP SIP, that were detected and resolved already in earlier versions. In conjunction with OBSO-1501-01 we recommend all customers to upgrade to the latest version (currently V3 R3.32.0) at the earliest opportunity.

## Vulnerability Details

**1. Input Validation Vulnerability (CVE-2014-9563)**
The SSH configuration in the web-based management interface (WBM) of OpenStage / OpenScape Desk Phone IP SIP in V3 before V3 R3.32.0 contains an input validation vulnerability (as defined in the Common Weakness Enumeration CWE-20). Successful exploitation requires to logon remotely at the WBM with administrator privileges ("admin" account) first. An attacker may then be able to modify the phone's root password. This password may be used in a later local attack to access the phone's debug port via the serial interface.

Note that the admin account also provides an alternate (legitimate) way to modify the configuration of the serial interface; therefore, the impact and risk is rated as low. A thorough security review has not unveiled any additional attack vectors through this input validation vulnerability.

**CVSS scores:**

- Base Score: 4.0
- Temporal Score 3.0
- CVSS v2 Vector (AV:N/AC:L/Au:S/C:N/I:P/A:N/E:U/RL:OF/RC:C)

Customer installations where the WBM interface is disabled on the phones are not affected by this vulnerability.

Mitre (cve.mitre.org) has assigned the id **CVE-2014-9563** to this issue.

**Credits to**: Martin Schobert and Thorsten Schröder (modzero AG Switzerland) for discovery, reporting and the coordinated analysis and disclosure of this vulnerability.

**2. Additional Vulnerability Reports**
modzero AG also reported additional vulnerabilities that were already detected earlier and independently during regular security tests in accordance with Unify's Baseline Security Policy. They have been resolved as follows:

**2.1 Improper default file access permissions**
Improper default file access permissions (as defined in CWE-276) allowed a legitimate low privileged Secure Shell (SSH) user ('admin') on the phone to gain superuser ('root') privileges on the phone. This vulnerability is only relevant when SSH access is (temporarily) enabled for diagnostic purposes.
The vulnerability is fixed in:

- OpenStage SIP: V3 R1.49.0 (release date: 2013-11-15) or later
- OpenScape Desk Phone IP SIP: V3 R2.16.0 (release date: 2013-12-12) or later

**2.2. Weak Session IDs**
The seed for the random generator that is used to generate session IDs for the Web-based management interface (WBM) provided insufficient entropy (as defined in CWE-331). An attacker could predict valid session IDs to hijack other users' WBM sessions. This vulnerability is only relevant when the WBM interface is enabled and actively used by legitimate administrators or end-users.
The vulnerability is fixed in:

- OpenStage SIP: V3 R0.48.0 (release date: 2011-09-30) or later
- OpenScape Desk Phone IP SIP: all versions

## Affected Products

- OpenStage / OpenScape Desk Phone IP SIP V3 all versions before V3 R3.32.0

## Recommended Actions

In conjunction with the high risk vulnerability described in OBSO-1501-01 we recommend to upgrade to the latest version (currently V3 R3.32.0, release date: 2015-01-16) at the earliest opportunity.

In the context of the issues described in this advisory, the following measures are generally recommended for secure operation of OpenStage and OpenScape Desk Phone IP phones:

- establish best-practice security measures for your VoIP environment, esp. ensure that VoIP devices are operated and managed in a separate VLAN
- install the latest ("up-to-date") available phone software
- deactivate the web-based management (WBM), if not used (use the OpenScape Deployment Service or an alternate central provisioning service instead)
- if the WBM is required:
  - configure a password policy and set appropriately strong passwords
  - import and activate a phone-individual SSL/TLS certificate for the WBM's https web server
- when (temporarily) activating the Secure Shell interface for diagnostic purposes, select a strong one-time password for access and set a short time limit (to automatically disable access after the specified time)

A comprehensive list of hardening recommendations can be found in the planning guide "OpenScape Desk Phone IP / OpenStage SIP V3R3 Security Checklist"

## References

Mitre:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9563
- CWE-20, CWE-276, CWE-331

Unify:

- Related Security Advisory OBSO-1501-01
- OpenScape Desk Phone IP / OpenStage SIP V3R3 Security Checklist

## Revision History

2015-02-26: Initial release

Advisory ID: OBSO-1501-02 (a=99), 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
obso@unify.com

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.