



## Security Advisory Report - OBSO-1410-01

### OpenStage / OpenScape Desk Phone IP - Authentication Bypass Vulnerability in web-based management (CVE-2014-7950)

Creation Date: 2014-10-10

Last Update: 2014-10-10

#### Summary

The web-based management interface of OpenStage / OpenScape Desk Phone IP (SIP V3 R3 before V3 R3.24.0 and HFA V3 before V3 R0.18.0) is vulnerable to authentication bypass. Attackers may get read and write access to the interface on administrative level.

The risk is rated **high**.

#### Vulnerability Details

The web-based management interface of OpenStage / OpenScape Desk Phone IP is vulnerable to authentication bypass (according to [CWE-302](#)). The vulnerability is due to insufficient session cookie validation.

Successful exploitation results in unauthorized access to administrative functions. This may lead to several types of attacks, including but not limited to: restart or factory reset of the phone, reconfiguration of the phone's network or server interfaces, upload of arbitrary files from a remote ftp server, redirection of the provisioning interface to a rogue Deployment Service.

Customer installations where the web-based management interface is disabled on the phones are not affected by this vulnerability.

CVSS Scores:

Base Score: 9.0, Temporal Score: 7.4

(AV:N/AC:L/Au:N/C:P/I:P/A:C/E:F/RL:OF/RC:C)

Mitre ([cve.mitre.org](http://cve.mitre.org)) has assigned the id CVE-2014-7950 to this issue.

This vulnerability was found internally during regular security tests in accordance with Unify's Baseline Security Policy.

#### Affected Products

- OpenStage / OpenScape Desk Phone IP SIP V3 R3 after V3 R3.9.0 and before V3 R3.24.0
- OpenStage / OpenScape Desk Phone IP HFA V3 before V3 R0.18.0

SIP: Earlier minor release versions (V3 R0, R1, R2) are not affected by CVE-2014-7950. However, note that these versions

- have already achieved End of SW support
- are vulnerable to e.g. CVE-2014-2650 (see Unify Security Advisory [OBSO-1403-01](#))

It is therefore recommended to update all SIP phones to V3 R3.24.0 or later - especially in environments where the web-based management interface cannot be disabled.

#### Recommended Actions

Install the following product releases (or later versions) to resolve the vulnerability:

- OpenStage / OpenScape Desk Phone SIP: V3 R3.24.0 (release date: 2014-10-10)
- OpenStage / OpenScape Desk Phone HFA: V3 R0.18.0 (release date: 2014-09-18)

Evaluate if the web-based management on the phones is not used and can therefore be disabled: this is a general security hardening recommendation and will also protect from potential exploitation of this particular vulnerability.

## References

Unify:

- Security Advisory [OBSO-1403-01](#)

Mitre:

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7950>
- [Common Weakness Enumeration #302](#)

## Revision History

2014-10-10: Initial release

---

Advisory ID: OBSO-1410-01 (a=89), 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](mailto:obs@unify.com)

© Unify Software and Solutions GmbH & Co. KG 2014

Mies-van-der-Rohe Str. 6, D-80807 München

[www.unify.com](http://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.