Security Advisory Report - OBSO-1403-01

OpenStage / OpenScape Desk Phone IP (SIP) - OS command injection vulnerability in web-based management (CVE-2014-2650)

Creation Date:	2014-03-28
Last Update:	2014-03-28

Summary

The web-based management interface of OpenStage / OpenScape Desk Phone IP SIP before V3 R3.11.0 is vulnerable to an OS command injection that could allow an unauthenticated remote attacker to execute arbitrary commands on the phone.

The risk is rated **high.**

Vulnerability Details

The vulnerability is due to insufficient input validation.

A phone is **not** affected if the web-based management interface (port https/443) is disabled.

CVSS Scores:

- Base Score 10.0, Temporal Score 8.7
(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Mitre (cve.mitre.org) has assigned the id CVE-2014-2650 to this issue.

Affected Products

The following VoIP phones of Unify are affected:

- OpenStage SIP V3, all models
- OpenScape Desk Phone IP SIP V3, all models

Not affected are:

- OpenStage SIP versions before V3
(Note however, that versions before V3 have already achieved End of Support)
- OpenStage HFA / OpenScape Desk Phone IP HFA

Recommended Actions

Install the following release (or later versions) on all OpenStage / OpenScape Desk Phone IP SIP phones at the earliest opportunity:

- V3 R3.11.0, release date: 2014-03-28

General recommendation: evaluate the possibility to disable the Web-based management on the VoIP Phones. This adds an additional layer of security by reducing the attack surface on VoIP phones.

References

CVE ID: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2650

Revision History

2014-03-28: Initial 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.