



Security Advisory Report - OBSO-1407-03

OpenStage / OpenScape Desk Phone IP - Information Exposure Vulnerability in web-based management

Creation Date: 2014-07-24
Last Update: 2014-07-24

Summary

The web-based management interface of OpenStage / OpenScape Desk Phone IP phones (SIP V3 before V3 R3.17.0 and HFA V3 before V3 R0.16.0) is vulnerable to information exposure that allows non-privileged users to view (but not modify) portions of admin controlled data.

The risk is rated as medium.

Vulnerability Details

The web-based management interface of OpenStage / OpenScape Desk Phone IP SIP in V3 is vulnerable to information exposure (according to the definition of Common Weakness Enumeration [CWE-200](#)). By using specially crafted URLs, the non-privileged user's logon/password is sufficient to view (but not modify) portions of administration data, that is restricted to the admin account only.

CVSS v2 Base Score: 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

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

Affected Products

- OpenStage SIP V3 / OpenScape Desk Phone IP SIP V3
- OpenStage HFA V3 / OpenScape Desk Phone IP HFA V3

Recommended Actions

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

- OpenStage SIP V3 / OpenScape Desk Phone SIP: V3 R3.17.0 (release date: 2014-07-18)
- OpenStage HFA V3 / OpenScape Desk Phone HFA: V3 R0.16.0 (release date: 2014-05-31)

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

External link (Mitre.org): [Common Weakness Enumeration #200](#)

Revision History

2014-07-24: Initial release

Advisory ID: OBSO-1407-03 (a=78), 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
obsso@unify.com
© Unify Software and Solutions GmbH & Co. KG 2014
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.