Security Advisory Report - OBSO-1403-02

OpenStage / OpenScape Desk Phone IP - Authentication Bypass Vulnerability in WPI Default Mode (CVE-2014-2651)

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

Summary

A vulnerability in the Default Mode of the WPI (Workpoint Interface) implementation in OpenStage and OpenScape Desk Phone IP SIP before V3 R3.11.0 allows unauthorized remote attackers to bypass a legitimate provisioning service (such as the OpenScape Deployment Service - DLS).

The risk is rated

- **high** for SIP in versions V3 before V3 R3.11.0
- low for SIP in versions < V3
- low for OpenStage HFA

A phone is **not** affected if it is operated in Secure Mode of the WPI.

Vulnerability Details

In Default Mode of the WPI, OpenStage and OpenScape Desk Phone IP phones only connect to the legitimate provisioning service (DLS) as configured in the associated DHCP configuration (vendor class "OptiIpPhone", option OpenStage.dls "sdlp://<dls-ip-address>:18443"). By sending a specially crafted https request, attackers may however be able to direct a phone to a different IP address than provided in the DHCP configuration. This may enable a rogue DLS to reconfigure the phone.

Phone versions V2 Rx.x.x are only affected with low impact: attackers may only be able to disconnect a phone from the legitimate DLS, but not to redirect them to a rogue DLS; the situation can be resolved from either the legitimate DLS server side, or by restarting the phone.

CVSS Scores:

- SIP V3: Base Score 9.3, Temporal Score 7.7
  (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)
- SIP/HFA V2: Base Score 2.9, Temporal Score 2.6
  (AV:A/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:W/RC:C)

Mitre (cve.mitre.org) has assigned the id CVE-2014-2651 to this issue.

Affected Products

The following VoIP phones of Unify are affected with high risk:

- OpenStage SIP V3, all models except OpenStage 5
- OpenScape Desk Phone IP SIP V3, all models

The following VoIP phones of Unify are affected with low risk:

- OpenStage HFA V2
- OpenStage SIP V2. Note that OpenStage SIP V2 has already achieved End of Support.

OpenStage HFA V3 is not affected.

Recommended Actions

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

- OpenStage / OpenScape Desk Phone IP SIP: V3 R3.11.0 (release date: 2014-03-28)
- OpenStage HFA: V2 R1.5.1 (release date: 2014-03-28)

General recommendation: evaluate the possibility to enable Secure Mode at the WPI between the Phones and the provisioning service (DLS). This adds an additional layer of security by certificate-based authentication of the service at the TLS protocol level.

References

CVE ID: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2651

Configuration of the Provisioning Interface (WPI): http://wiki.unify.com/images/c/c7/OpenStage_Provisioning_Interface_Developer%27s_Guide.pdf

Revision History

Initial release: 2014-03-28

Advisory ID: OBSO-1403-02 (a=65), 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.
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.