Security Advisory Report - OBSO-1501-01

OpenStage / OpenScape Desk Phone IP - Authentication Bypass Vulnerability in WPI Default Mode (CVE-2015-1184)

Creation Date: 2015-01-20
Last Update: 2015-03-24

Summary

A vulnerability in the Default Mode of the WPI (Workpoint Interface) implementation in OpenStage and OpenScape Desk Phone IP (both SIP and HFA variants) allows unauthorized remote attackers to bypass a legitimate provisioning service (such as the OpenScape Deployment Service - DLS).
Note that this is a similar, but different vulnerability than CVE-2014-2651 (OBSO-1403-02 as reported on 2014-03-28).

The risk is rated **high** for

- SIP V3 R3.17.0, V3 R3.17.1, V3 R3.17.2 and V3 R3.24.0
- HFA V3 R0.18.0 and V3 R0.18.2

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.

CVSS Scores:

- SIP V3 R3: 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)
- HFA V3 R0: Base Score 9.3, Temporal Score 8.4
  (AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:W/RC:C)

Mitre (cve.mitre.org) has assigned the id CVE-2015-1184 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 R3.17.x and V3 R3.24.x
- OpenStage / OpenScape Desk Phone IP HFA V3 R0.18.x

Older versions are not affected by this vulnerability. This includes:

- OpenStage / OpenScape Desk Phone IP SIP before V3 R3.17.0
- all prior minor releases of the SIP variant V3 R0/R1/R2
- OpenStage / OpenScape Desk Phone IP HFA V3 R0.16.x and earlier

Recommended Actions

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

- OpenStage / OpenScape Desk Phone IP SIP (all existing phone models): V3 R3.32.0 (release date: 2015-01-16)
- New phone model OpenScape Desk Phone IP 35G Eco SIP: V3 R3.33.0 (release date: 2015-01-16)
- OpenStage / OpenScape Desk Phone IP HFA: V3 R0.23.0 (release date: 2015-03-16)

General recommendations:

- 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
- establish best-practice security measures for your VoIP environment, esp. ensure that VoIP devices are operated and managed in a separate VLAN

References

Unify:

- Related Security Advisory: OBSO-1403-02

Mitre:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1184

Revision History

2015-01-20: Initial release

2015-03-18: Update 01

- Fix release for OpenStage HFA available

2015-03-24: Update 02

- Corrected and completed the list of affected and unaffected OpenStage and Desk Phone IP versions

Advisory ID: OBSO-1501-01 (a=98), status: update 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