



Security Advisory Report - OBSO-1505-02

OpenStage / OpenScape Desk Phone IP - HTTP header parsing vulnerability (CVE-2014-9708)

Creation Date: 2015-05-08

Last Update: 2015-08-13

Summary

The Webserver (https/443) interface of OpenStage / OpenScape Desk Phone IP (SIP and HFA) contains a flaw in the HTTP header parsing that could allow a remote unauthenticated attacker to cause a temporary DoS (Denial of Service) condition for the legitimate user(s) of the phone.

The risk is rated **medium**.

Vulnerability Details

As published in [CVE-2014-9708](#), Embedthis Appweb web server is prone to a denial-of-service vulnerability due to a null-pointer dereference condition (as defined in the Common Weakness Enumeration [CWE-476](#)) when parsing HTTP Range headers. A remote attacker could exploit this issue using an HTTP request with an empty range value and cause a denial-of-service condition.

OpenStage / OpenScape Desk Phone IP use a vulnerable version of Embedthis Appweb web server at the https interface (port 443). Successful exploitation could result in a reboot, causing a temporary DoS (Denial of Service) condition for the legitimate user(s) of the phone.

The risk is rated as medium, but note that

- the vulnerability and all details how to exploit it are publicly known (see chapter "References")
- mitigation measures are not available (see chapter "Recommended Actions")

CVSSv2 scores:

- Base Score: 5.0
- Temporal Score 4.1
- CVSS v2 Vector ([AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C](#))

CVSSv3 scores:

- Base Score: 5.3
- Temporal Score 4.9
- CVSS v3 Vector ([AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:F/RL:O/RC:C](#))

Affected Products

- OpenStage / OpenScape Desk Phone IP SIP V3, all versions before V3 R3.36.1
- OpenStage / OpenScape Desk Phone IP HFA V3, all versions before V3 R0.23.2

Recommended Actions

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

- OpenStage / OpenScape Desk Phone SIP: V3 R3.36.1 (release date: 2015-05-08)
- OpenStage / OpenScape Desk Phone HFA: V3 R0.23.3 (release date: 2015-08-13)
Note that the correction is also available in V3 R0.23.2, but this version did not achieve GA (general availability)

Mitigation measures are not available.

Note that disabling the web-based management interface is not effective in this case, as the web service (https/443) remains open to serve contact-me requests for the Workpoint Interface (WPI) from provisioning systems such as the OpenScape Deployment Service.

References

- [NIST/NVD vulnerability entry for CVE-2014-9708](#)
- [Embedthis appweb statement](#)
- [Public disclosure of CVE-2014-9708](#)
- [CWE-476](#)

Revision History

2015-05-08: Initial release

2015-08-13: Update 01

- Fix version for OpenStage / OpenScape Desk Phone HFA now also available
- Added CVSSv3 Scores (according to CVSSv3 specification released by FIRST in June 2015 (<https://www.first.org/cvss>))

Advisory ID: OBSO-1505-02 (a=108), 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

© Unify Software and Solutions GmbH & Co. KG 2015

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.