Security Advisory Report - OBSO-1312-01

OpenStage HFA/SIP - Cross-site scripting vulnerability in web-based management

Creation Date: 2013-12-16
Last Update: 2013-12-16

Summary

OpenStage SIP and HFA phones are vulnerable to a cross-site scripting attack in the web-based management (WBM) user interface. The risk is rated as "medium".

Customers are therefore advised to perform the "Recommended Actions" at the earliest opportunity.

Vulnerability Details

The vulnerability could be exploited by attackers through:

- logging on as user on the phone's WBM
- creation of arbitrary softkey label names containing malicious JavaScript code
- tricking a victim person (esp. administrators) into logging on the phone's WBM and view the softkey configuration page; malicious code may be executed on the victim's system

Affected Products

- OpenStage SIP V3 R1
  (later versions of OpenStage or Desk Phone IP are not affected)
- OpenStage HFA V2 R0
- OpenStage HFA V2 R1

Recommended Actions

Upgrade to the following versions (or later) of OpenStage phones to close this vulnerability:

- OpenStage SIP V3 R1.41.0 (released on: 2013-03-01)
- OpenStage HFA V2 R0.98.0 (release date: 2013-09-03)
- OpenStage HFA V2 R1.5.0 (release date: 2013-12-13)

Independent of this particular threat, many general countermeasures to mitigate such types of attacks are recommended and documented in the Security Checklist (hardening guide) for OpenStage phones. For example:

- Disable the WBM if not in use (available in V3 only)
- Let phone users chose individual and complex passwords for authentication
- Avoid that administrators are using the WBM for administrative tasks; instead use a centralized solution, preferably via OpenScape Deployment Service (DLS) or similar provisioning system. Besides the obvious cost savings (by avoiding time consuming and error-prone phone-individual configuration), this also has significant benefits in the secure management of a large number of VoIP phones (such as the support of roles/access rights, accountability, logging of the action taken by individual administrators etc.).

References

N.A.

Revision History

2013-12-16: Initial release

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.