



Security Advisory Report - OBSO-1011-01

OpenStage - configuration data readable by unauthorized users

Creation Date: 2010-11-30

Last Update: 2010-11-30

Summary

Two vulnerabilities in the web-based management of OpenStage SIP and HFA were reported, which allow to download parts of the phone's configuration data and to upload files onto the phone without authentication.

Vulnerability Details

A vulnerability in the web-based management of OpenStage SIP and HFA allows to download parts of the configuration data on the phone without authentication. A specially crafted URL can be used to bypass the admin login and download phone data like the user's phonebook or key settings.

Another specially crafted URL allows to upload arbitrary files onto the phone. However, up to now no possibility is known to take over control of the phone by specially crafted files.

The non-IP phone variant OpenStage TDM is also affected, when the IP over USB interface is used. There is significant lower risk with TDM phones, since this requires physical access to the phone using USB cable.

Affected Products

- OpenStage SIP: V1 all versions, V2 < V2 R1.21.0
- OpenStage HFA: V1 all versions, V2 < V2 R0.48.0
- OpenStage TDM: V1 all versions, V2 < V2 R0.44.0

Recommended Actions

We recommend customers to upgrade OpenStage phones to at least the following versions:

- OpenStage SIP: V2 R1.21.0
- OpenStage HFA: V2 R0.48.0
- OpenStage TDM: V2 R0.44.0

Note that OpenStage V1 has already reached end of SW support; please consider an upgrade to the latest V2 version.

References

None.

Revision History

2010-11-30: Initial release

Advisory ID: OBSO-1011-01 (a=7), 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

obs@unify.com

© Unify Software and Solutions GmbH & Co. KG 2010

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.