Security Advisory Report - OBSO-1108-01

OpenStage - password accessible in cleartext on webbased interface

Creation Date: 2011-08-22
Last Update: 2011-08-22

Summary

A vulnerability in the web-based management of OpenStage SIP was reported, which allows to read the currently configured passwords (e.g. for SIP registration) in cleartext.

Vulnerability Details

The vulnerability affects various passwords that can be set as configuration parameters via the web-based management interface of both OpenStage SIP and OpenStage HFA variants.

Note that exploitation of this vulnerability requires being logged on as admin in the phone's web-based management access.

The risk level is considered low: to gain knowledge about configured passwords, attackers first need to compromise administrators' browsers, then tricking them to open the web-based management and access the relevant sites. In customer environments, where the administration of OpenStage phones is done solely through a central administration tool (esp. OpenScape Deployment Service), the vulnerability is not relevant at all.

Affected Products

- OpenStage SIP: V1 all versions; V2 R0, V2 R1
- OpenStage HFA: V1 all versions; V2 R0

OpenStage TDM is not affected by this vulnerability.

Recommended Actions

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

- OpenStage SIP: V2 R1.28.0, any V2 R2 version, or higher
- OpenStage HFA: V2 R0.57.0 or higher

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

References

None.

Credits to Karim Elmaizi who had discovered and reported this vulnerability.

Revision History

2011-08-22: Initial release

Advisory ID: OBSO-1108-01 (a=20), 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