Security Advisory Report - OBSO-1402-01

Mediatrix VoIP Gateways - Cross-site scripting (XSS) vulnerability - CVE-2014-1612

Creation Date: 2014-02-07
Last Update: 2014-02-07

Summary

A cross-site scripting (XSS) vulnerability was detected and reported for Media5's Mediatrix VoIP Gateways.
The risk is medium (CVSSv2 Base Score 4.3).

We recommend customers of Unify that use Mediatrix Gateways to verify their gateways' firmware version and upgrade to the latest version as released for use in OpenScape solutions.

Vulnerability Details

A cross-site scripting (XSS) vulnerability in login.esp in the Web Management Interface in Media5 Mediatrix VoIP Gateway with firmware Dgw 1.1 (all versions) and Dgw 2.0 (before 2.0.20.301) allows remote attackers to inject arbitrary web script or HTML via the username parameter.

cve.mitre.org has assigned the name CVE-2014-1612 to this issue

Risk: medium
CVSSv2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Affected Products

Mediatrix VoIP Gateways:

- 44xx series
- 41xx series
- 36xx series

Recommended Actions

Unify customers should upgrade to latest approved GA version available at Unify's Software Download Server (SWS).
Currently, this is version V2.0 R26.451.0.

References

- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1612
- NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-1612
- OSVDB: http://osvdb.org/102415

Revision History

2014-02-07: Initial release

Advisory ID: OBSO-1402-01 (a=73), 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
© Unify Software and Solutions GmbH & Co. KG 2014
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.