Security Advisory Report - OBSO-1306-01

OpenScape Branch / OpenScape SBC - Multiple Web Interface Vulnerabilities

Creation Date: 2013-06-12
Last Update: 2013-11-08

Summary

OpenScape Branch and OpenScape SBC contain four vulnerabilities that may result in an unauthenticated, remote attacker to cause a denial of service or otherwise hack into the server, in the worst case.

Unify has released software updates that resolve these vulnerabilities.

Vulnerability Details

The four vulnerabilities are classified as:

- high risk: OS command execution vulnerability
- medium risk: path traversal vulnerability
- medium risk: non-permanent cross-site scripting vulnerability
- low risk: information disclosure

To avoid potential risks of attacks, confidentiality concerns and in order to expedite the process, no vulnerability details are disclosed.

Affected Products

- OpenScape Branch, all versions
- OpenScape SBC, all versions

Recommended Actions

We recommend that customers upgrade to at least the following versions:

- OpenScape Branch: V2 R0.32.0 or V7 R1.7.0
- OpenScape SBC: V2 R0.32.0 or V7 R1.7.0

Customers with OpenScape Branch V1 R4, should upgrade to V2 or higher.
If a customer is unable to upgrade as recommended at this time, an upgrade to at least V1 R4.17.0 will reduce the risk level of the OS command execution vulnerability from high to medium: All unresolved issues in V1 R4.17.0 require prior authentication. Please follow the recommendations in the Security Checklist of OpenScape Branch/SBC how to harden the access to the web interface, esp. configuring individual and complex passwords for all enabled accounts.

References

None.

Credits to

- S. Viehböck, M. Heinzl and F. Lukavsky of the SEC Consult Vulnerability Lab, Vienna, who had discovered and reported the vulnerabilities as part of a customer security audit
- the relevant customer for sharing the details of the security audit with us

Revision History

2013-06-12: Initial release
2013-11-08: Rereleased under the Unify brand (formerly Siemens Enterprise Communications)

Advisory ID: OBSO-1306-01 (a=53), 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

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com