



## Security Advisory Report - OBSO-1307-02

### OpenScape Branch/SBC - Nameserver vulnerabilities (CVE-2012-4244, CVE-2012-5166, CVE-2013-2266)

Creation Date: 2013-07-26  
Last Update: 2013-07-26

#### Summary

OpenScape Branch (OSB) V7 R1.9.0 and OpenScape Session Border Controller (SBC) V7 R1.9.0 are released to address three security vulnerabilities in its nameserver ('named' process). The vulnerabilities are rated as "high" in the context of OSB/SBC.

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

#### Vulnerability Details

OpenScape Branch/SBC are affected by the following Denial-of-Service vulnerabilities:

- **CVE-2012-4244:** The 'named' process could be caused to exit with a REQUIRE exception if it can be induced to load a specially crafted resource record
- **CVE-2012-5166:** When specific combinations of RDATA are loaded into OSB/SBC's nameserver, either via cache or an authoritative zone, a subsequent query for a related record may cause the 'named' process to lock up
- **CVE-2013-2266:** A flaw in the bind library when processing regular expressions may allow a remote attacker to deliberately cause excessive memory consumption by the 'named' process

Refer to the references given below for more details.

Note that OSB/SBC are **not** affected by other vulnerabilities, as recently reported for the nameserver (BIND) component (CVE-2013-3919, CVE-2012-5689, CVE-2012-5688).

#### Affected Products

- OpenScape Branch V7
- OpenScape Session Border Controller V7

#### Recommended Actions

Upgrade to **OpenScape Branch/OpenScape SBC V7 R1.9.0** or higher to address these vulnerabilities.

For details refer to the Release Notes of OSB V7 R1.9.0 (release date: 2013-07-24) and of SBC V7 R1.9.0 (release date: 2013-07-24).

#### References

Internet Systems Consortium (ISC):

- CVE-2012-4244: <https://kb.isc.org/article/AA-00778>
- CVE-2012-5166: <https://kb.isc.org/article/AA-00801>
- CVE-2013-2266: <https://kb.isc.org/article/AA-00871>

Mitre:

- CVE-2012-4244: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4244>
- CVE-2012-5166: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5166>
- CVE-2013-2266: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2266>

#### Revision History

2013-07-26: Initial release

---

Advisory ID: OBSO-1307-02 (a=58), 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](mailto:obs@unify.com)

© Unify Software and Solutions GmbH & Co. KG 2013

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

[www.unify.com](http://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.