UNIFY

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

Contact and Disclaimer