Security Advisory Report - OBSO-1307-01

OpenScape Voice V7 R1 - Multiple Vulnerabilities in Operating System and Java Components

Creation Date: 2013-07-24
Last Update: 2013-12-06

Summary

OpenScape Voice V7 R1 has released the Method Of Procedure (MOP) **P30310-Q3018-Q170-*-7620** to address critical security vulnerabilities in the Operating System and Java components.

Since some of the vulnerabilities are rated as "high" in the context of OpenScape Voice, customers are advised to perform the "Recommended Actions" at the earliest opportunity.

The advisory also applies in the same way to all installations of OpenScape Enterprise Express V7 R1.

Update 2013-12-06:
A bug in the Linux kernel update, that was delivered with the previous MOP P30310-Q2944-Q170-*-7620 (IPSec packet corruption causing call failures) affected a very limited set of OpenScape Voice installations, so these had to deinstall the MOP.
A new MOP P30310-Q3018-Q170-*-7620 has now been released as part of various hotfix versions of OpenScape Voice. We recommend **all** customers (incl. those who were not affected by the linux kernel bug) to update to one of these hotfix versions, or later, since an additional critical update is contained as well (CVE-2013-4854).

Vulnerability Details

The table below provides an overview of all vulnerabilities relevant to OpenScape Voice (OSV) V7 R1 that were solved with**P30310-Q3018-Q170-*-7620.**

Note: the associated vendor advisories may also include solutions for various other vulnerabilities (identified through different CVE numbers). However, these additional corrections are not relevant in the context of OpenScape Voice and therefore not listed here.

Vulnerability ID (ref. to cve.mitre.org)	**Description**	**Impact to OSV V7 R1**	**Risk Level**	**Vendor Advisory and Details**
Operating System (Novell SLES):				
New in Q3018: CVE-2013-4854	ISC BIND: Denial of service vulnerability	Remote attackers may cause a denial of service (crash the DNS service via specially crafted query) on OSV.	high	CVE-2013-4854
CVE-2013-2850	Linux kernel: Heap-based buffer overflow in the iSCSI target subsystem	Remote attackers may cause a denial of service (memory corruption and OOPS) or possibly execute arbitrary code on OSV.	high	CVE-2013-2850
CVE-2012-4505	libproxy: Heap-based buffer overflow in px_pac_reload function in lib/pac.c	If OSV is configured with PAC proxy configuration, a remote malicious server or a man-in-the-middle attacker may cause libproxy on OSV to crash or possibly execute arbitrary code on OSV.	high	CVE-2012-4505
CVE-2012-5134	libxml2: Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c	A remote attacker could provide a specially-crafted XML file that, could cause an OSV application to crash or possibly execute arbitrary code.	medium	CVE-2012-5134
CVE-2012-3418 et.al.	Performance Co-Pilot (pcp): multiple vulnerabilities	A remote attacker could cause a denial of service and possibly execute arbitrary code on OSV.	medium	openSUSE Advisory
CVE-2012-5611 et.al.	mysql-libraries: stack-based	Remote authenticated users	medium	openSUSE Advisory

	buffer overflow in the acl_get function and various other - less critical - vulnerabilities	may execute arbitrary code on OSV.		
CVE-2013-0871	Linux kernel: Race condition in the ptrace functionality	A local user on OSV may gain superuser privileges.	medium	CVE-2013-0871
CVE-2013-1667	Perl: Denial of service vulnerability in the rehashing code implementation	An attacker may provide specially-crafted input to be used as hash keys by a Perl application, which could cause excessive memory consumption on the OSV server.	medium	CVE-2013-1667
CVE-2013-1653 et. al.	Puppet: Various vulnerabilities, CVE-2013-1653 is the most critical one	When OSV is managed via Puppet configuration management, remote users may exceute arbitrary code on the OSV.	medium	openSUSE Advisory
CVE-2013-1767 et. al.	Linux kernel: Multiple vulnerabilities exploitable by local users	The vulnerabilities allow local users on OSV to • Run arbitrary code with root privileges on OSV (CVE-2013-1767, CVE-2013-0268) • Cause a denial of service (CVE-2012-2137, CVE-2013-1772, CVE-2013-1792) • Obtain sensitive information (CVE-2012-6549, CVE-2012-6548, CVE-2013-2634, CVE-2013-2635)	medium	openSUSE Advisory
CVE-2013-2094	Linux kernel: Use of incorrect integer data type in the perf_swevent_init function.	A local user may gain root privileges on OSV via crated perf_event_open system call. *Note that this vulnerability is considered high risk on general purpose linux systems, while on OSV the risk is only medium.*	medium	CVE-2013-2094
IBM:				
CVE-2013-1537	Java Runtime Environment (JRE): vulnerability in the RMI component	The vulnerability may enable an attacker to load arbitrary code onto the OSV	high	CVE-2013-1537
CVE-2013-0440	JRE: vulnerability in the JSSE component, allowing an unlimited number of handshake restarts	A remote attacker could make JRE-based TLS services on OSV consume an excessive amount of CPU by continuously restart the handshake.	medium	CVE-2013-0440
CVE-2013-0169	JRE: SSL/TLS Plaintext Recovery vulnerability ("Lucky 13")	Attackers may recover plaintext from a TLS encrypted communication link by exploiting timing differences that arise during processing of TLS message authentication codes (MAC).	medium	CVE-2013-0169
CVE-2012-5081	JRE: unspecified vulnerability in the JSSE component	A remote attacker could enforce a denial-of-service condition for JRE-based TLS services on OSV.	medium	CVE-2012-5081
CVE-2012-3329	Advanced Settings Utility (ASU): vulnerability related to temporary file or log file creation	A local attacker may create malicious file links on the OSV server that could corrupt the Operating System.	low	CVE-2012-3329

Affected Products

- OpenScape Voice V7 R1
- OpenScape Enterprise Express V7 R1

Recommended Actions

Install one of the following Hotfix releases (or later versions) on OpenScape Voice V7 R1/OpenScape Enterprise Express at the earliest opportunity:

- V7 R1.33.4 (Cumulative), release date: 2013-12-02
- V7 R1.30.8 (Cumulative), release date: 2013-11-19
- V7 R1.21.17 (Cumulative), release date: 2013-12-06

References

Relevant references to vendor advisories (Novell, IBM) and to Mitre are given in table in the section "Vendor Advisory and Details".

Revision History

2013-07-24: Initial release
2013-12-06: Update release: new MOP/Hotfix releases of OpenScape Voice available

Advisory ID: OBSO-1307-01 (a=62), 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

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.