Security Advisory Report - OBSO-1401-01

OpenScape Voice V6 - Multiple Vulnerabilities in Operating System and Java Components

Creation Date: 2014-01-15
Last Update: 2014-01-15

Summary

OpenScape Voice V6 has released V6 R0.24.6 to address various security vulnerabilities in the Operating System distribution and in the Java components.

None of the vulnerabilities are rated as "high" in the context of OpenScape Voice. Nevertheless, customers are advised to perform the "Recommended Actions" at the earliest opportunity.

Vulnerability Details

The table below provides an overview of all vulnerabilities relevant to OpenScape Voice (OSV) V6 that were solved with the Method Of Procedure (MOP) **P30310-Q3026-Q160-*-7620** as included in the fix release V6 R0.24.6.

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 V6**	**Risk Level**	**Vendor Advisory and Details**
Novell Suse Linux Enterprise Server:				
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-2013-0338	libxml2: denial of service vulnerability via an XML file containing an entity declaration with long replacement text and many references to this entity, aka "internal entity expansion" with linear complexity.	A remote attacker could provide a specially-crafted XML file that could cause an OSV application to crash.	low	CVE-2013-0338
CVE-2013-1667	Perl: Denial of service vulnerability in the rehashing code implementation	An remote 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-2013-4113	php: the xml parser does not properly consider parsing depth, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted document that is processed by the xml_parse_into_struct function.	A remote attacker could provide a specially-crafted XML file that could cause an OSV application to crash.	medium	CVE-2013-4113
CVE-2013-2116	GnuTLS: The _gnutls_ciphertext2compressed function in lib/gnutls_cipher.c allows remote attackers to cause a denial of service (buffer	A remote attacker could cause an OSV application or the SIP-TLS service to crash by manipulating TLS-encrypted data.	medium	CVE-2013-2116

	over-read and crash) via a crafted padding length.			
CVE-2013-0871, CVE-2013-0160	Linux kernel: Two vulnerabilities exploitable by local users	The vulnerabilities allow local users on OSV to • Run arbitrary code with root privileges on OSV (CVE-2013-0871) • Obtain sensitive information (CVE-0213-0160)	medium	CVE-2013-0871, CVE-2013-0160
IBM Java:				
CVE-2013-5372	Java Runtime Environment (JRE): vulnerability in the XML4J parser	A remote attacker could provide a specially-crafted XML file that could cause an OSV application to crash.	medium	IBM Security Update 11.2013
CVE-2013-4002, CVE-2013-5802	JRE: vulnerabilities in the JAXB and other components	A remote attacker could cause Java applications on OSV to crash or bypass certain security restrictions.	medium	IBM Security Update 10.2013

Affected Products

- OpenScape Voice V6

Recommended Actions

Install the following Hotfix release (or later versions) on OpenScape Voice V6 at the earliest opportunity:

- V6 R0.24.6, release date: 2014-01-08

References

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

Revision History

2014-01-15: Initial release

Advisory ID: OBSO-1401-01 (a=69), 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

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.