



CVE-2014-3683

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2014-3683
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-02 00:55:00 UTC
Updated	2016-10-18 03:44:00 UTC
Description	Integer overflow in rsyslog before 7.6.7 and 8.x before 8.4.2 and syslogd 1.5 and earlier allows remote attackers to cause

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rsyslog	Rsyslog	8.1.0	All	All	All
Application	Rsyslog	Rsyslog	8.1.1	All	All	All
Application	Rsyslog	Rsyslog	8.1.2	All	All	All
Application	Rsyslog	Rsyslog	8.1.3	All	All	All
Application	Rsyslog	Rsyslog	8.1.4	All	All	All
Application	Rsyslog	Rsyslog	8.1.5	All	All	All
Application	Rsyslog	Rsyslog	8.1.6	All	All	All
Application	Rsyslog	Rsyslog	8.2.0	All	All	All
Application	Rsyslog	Rsyslog	8.2.1	All	All	All
Application	Rsyslog	Rsyslog	8.2.2	All	All	All
Application	Rsyslog	Rsyslog	8.2.3	All	All	All
Application	Rsyslog	Rsyslog	8.3.0	All	All	All
Application	Rsyslog	Rsyslog	8.3.1	All	All	All
Application	Rsyslog	Rsyslog	8.3.2	All	All	All
Application	Rsyslog	Rsyslog	8.3.3	All	All	All
Application	Rsyslog	Rsyslog	8.3.4	All	All	All
Application	Rsyslog	Rsyslog	8.3.5	All	All	All

Application	Rsyslog	Rsyslog	8.4.0	All	All	All
Application	Rsyslog	Rsyslog	8.4.1	All	All	All
Application	Rsyslog	Rsyslog	8.1.0	All	All	All
Application	Rsyslog	Rsyslog	8.1.1	All	All	All
Application	Rsyslog	Rsyslog	8.1.2	All	All	All
Application	Rsyslog	Rsyslog	8.1.3	All	All	All
Application	Rsyslog	Rsyslog	8.1.4	All	All	All
Application	Rsyslog	Rsyslog	8.1.5	All	All	All
Application	Rsyslog	Rsyslog	8.1.6	All	All	All
Application	Rsyslog	Rsyslog	8.2.0	All	All	All
Application	Rsyslog	Rsyslog	8.2.1	All	All	All
Application	Rsyslog	Rsyslog	8.2.2	All	All	All
Application	Rsyslog	Rsyslog	8.2.3	All	All	All
Application	Rsyslog	Rsyslog	8.3.0	All	All	All
Application	Rsyslog	Rsyslog	8.3.1	All	All	All
Application	Rsyslog	Rsyslog	8.3.2	All	All	All
Application	Rsyslog	Rsyslog	8.3.3	All	All	All
Application	Rsyslog	Rsyslog	8.3.4	All	All	All
Application	Rsyslog	Rsyslog	8.3.5	All	All	All
Application	Rsyslog	Rsyslog	8.4.0	All	All	All
Application	Rsyslog	Rsyslog	8.4.1	All	All	All
Application	Rsyslog	Rsyslog	All	All	All	All
Application	Sysklogd Project	Sysklogd	1.1	All	All	All
Application	Sysklogd Project	Sysklogd	1.2	All	All	All
Application	Sysklogd Project	Sysklogd	1.3	All	All	All
Application	Sysklogd Project	Sysklogd	1.4	All	All	All
Application	Sysklogd Project	Sysklogd	1.4.1	All	All	All
Application	Sysklogd Project	Sysklogd	1.1	All	All	All
Application	Sysklogd Project	Sysklogd	1.2	All	All	All
Application	Sysklogd Project	Sysklogd	1.3	All	All	All
Application	Sysklogd Project	Sysklogd	1.4	All	All	All
Application	Sysklogd Project	Sysklogd	1.4.1	All	All	All
Application	Sysklogd Project	Sysklogd	All	All	All	All

References

Reference	Source	Link	Tags
USN-2381-1: Rsyslog vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	
oss-security - vulnerability in rsyslog	MLIST	www.openwall.com	
remote syslog PRI vulnerability – CVE: CVE-2014-3683	CONFIRM	www.rsyslog.com	Exploit, Patch, V
Debian -- Security Information -- DSA-3047-1 rsyslog	DEBIAN	www.debian.org	
openSUSE-SU-2014:1297-1: moderate: update for rsyslog	SUSE	lists.opensuse.org	
oss-security - syslogd vulnerability (CVE-2014-3634)	MLIST	www.openwall.com	Patch
Oracle Solaris Third Party Bulletin - October 2015	CONFIRM	www.oracle.com	
openSUSE-SU-2014:1298-1: moderate: update for rsyslog	SUSE	lists.opensuse.org	
[security-announce] SUSE-SU-2014:1294-1: important: Security update for	SUSE	lists.opensuse.org	
Security Advisory SA61494 - rsyslog PRI Two Buffer Overflow Vulnerabilities - Secunia	SECUNIA	secunia.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report