



CVE-2014-9761

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

Summary

CVE	CVE-2014-9761
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-19 21:59:00 UTC
Updated	2019-06-13 21:29:00 UTC
Description	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attacks

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Gnu	Glibc	All	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp4	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp2	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp3	All	All
Application	Suse	Linux Enterprise Debuginfo	11.0	sp4	All	All

Operating System	Suse	Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Server	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11.0	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp1	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	acce
[security-announce] SUSE-SU-2016:0470-1: important: Security update for	SUSE	lists.
Full Disclosure: SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series	FULLDISC	secli
oss-security - Re: CVE assignment request for security bugs fixed in glibc 2.23	MLIST	www

16962 – (CVE-2014-9761) nan function unbounded stack allocation (CVE-2014-9761)	CONFIRM	source
Bugtraq: SEC Consult SA-20190612-0 :: Multiple vulnerabilities in WAGO 852 Industrial Managed Switch Series	BUGTRAQ	secu
Adhemerval Zanella - The GNU C Library version 2.23 is now available	MLIST	www
USN-2985-2: GNU C Library regression Ubuntu	UBUNTU	www
Full Disclosure: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X	FULLDISC	secu
oss-security - CVE assignment request for security bugs fixed in glibc 2.23	MLIST	www
Cisco Device Hardcoded Credentials / GNU glibc / BusyBox ≈ Packet Storm	MISC	pack
[security-announce] SUSE-SU-2016:0472-1: important: Security update for	SUSE	lists
Bugtraq: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X	BUGTRAQ	secu
[security-announce] SUSE-SU-2016:0473-1: important: Security update for	SUSE	lists
[security-announce] openSUSE-SU-2016:0510-1: important: Security update	SUSE	lists
Red Hat Customer Portal	REDHAT	rhn
[SECURITY] Fedora 23 Update: glibc-2.22-15.fc23	FEDORA	lists
USN-2985-1: GNU C Library vulnerabilities Ubuntu	UBUNTU	www
[security-announce] SUSE-SU-2016:0471-1: important: Security update for	SUSE	lists
GNU C Library: Multiple vulnerabilities (GLSA 201702-11) — Gentoo security	GENTOO	secu
GNU glibc CVE-2014-9761 Stack Buffer Overflow Vulnerability	BID	www
WAGO 852 Industrial Managed Switch Series Code Execution / Hardcoded Credentials ≈ Packet Storm	MISC	pack
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710558](#) Gentoo Linux GNU C Library Multiple Vulnerabilities (GLSA 201702-11)

© 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](#)