



# CVE-2015-8778

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-8778
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-04-19 21:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Glibc</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp2	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp3	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp4	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp2	All	All

Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp3	All	All
Application	<a href="#">Suse</a>	<a href="#">Linux Enterprise Debuginfo</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Desktop</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp2	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Server</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	11	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	11	sp4	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise Software Development Kit</a>	12	sp1	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	12	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux Enterprise Server</a>	12	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
[security-announce] SUSE-SU-2016:0470-1: important: Security update for	SUSE	<a href="#">lists.</a>

oss-security - Re: CVE assignment request for security bugs fixed in glibc 2.23	MLIST	<a href="#">www</a>
GNU glibc 'misc/hsearch_r.c' Integer Overflow Vulnerability	BID	<a href="#">www</a>
Adhemerval Zanella - The GNU C Library version 2.23 is now available	MLIST	<a href="#">www</a>
USN-2985-2: GNU C Library regression   Ubuntu	UBUNTU	<a href="#">www</a>
Full Disclosure: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X	FULLDISC	<a href="#">secu</a>
oss-security - CVE assignment request for security bugs fixed in glibc 2.23	MLIST	<a href="#">www</a>
Cisco Device Hardcoded Credentials / GNU glibc / BusyBox ≈ Packet Storm	MISC	<a href="#">pack</a>
[security-announce] SUSE-SU-2016:0472-1: important: Security update for	SUSE	<a href="#">lists.</a>
Bugtraq: SEC Consult SA-20190904-0 :: Multiple vulnerabilities in Cisco router series RV34X, RV26X and RV16X	BUGTRAQ	<a href="#">secu</a>
18240 – (CVE-2015-8778) hcreate, hcreate_r should fail with ENOMEM if element count is too large (CVE-2015-8778)	CONFIRM	<a href="#">sour</a>
Debian -- Security Information -- DSA-3481-1 glibc	DEBIAN	<a href="#">www</a>
GNU C Library: Multiple vulnerabilities (GLSA 201602-02) — Gentoo Security	GENTOO	<a href="#">secu</a>
[security-announce] SUSE-SU-2016:0473-1: important: Security update for	SUSE	<a href="#">lists.</a>
[security-announce] openSUSE-SU-2016:0510-1: important: Security update	SUSE	<a href="#">lists.</a>
Red Hat Customer Portal	REDHAT	<a href="#">rhn.r</a>
[SECURITY] Fedora 23 Update: glibc-2.22-15.fc23	FEDORA	<a href="#">lists.</a>
USN-2985-1: GNU C Library vulnerabilities   Ubuntu	UBUNTU	<a href="#">www</a>
[security-announce] SUSE-SU-2016:0471-1: important: Security update for	SUSE	<a href="#">lists.</a>
Debian -- Security Information -- DSA-3480-1 eglibc	DEBIAN	<a href="#">www</a>
GNU C Library: Multiple vulnerabilities (GLSA 201702-11) — Gentoo security	GENTOO	<a href="#">secu</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.r</a>

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](#)