CVE-2014-6040

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-6040
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-05 16:59:00 UTC
Updated	2023-02-13 00:42:00 UTC
Description	GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.9	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All

Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12	All	All	All
Application	Gnu	Glibc	2.12.1	All	All	All
Application	Gnu	Glibc	2.12.2	All	All	All
Application	Gnu	Glibc	2.13	All	All	All
Application	Gnu	Glibc	2.14	All	All	All
Application	Gnu	Glibc	2.14.1	All	All	All
Application	Gnu	Glibc	2.15	All	All	All
Application	Gnu	Glibc	2.16	All	All	All
Application	Gnu	Glibc	2.17	All	All	All
Application	Gnu	Glibc	2.18	All	All	All
Application	Gnu	Glibc	2.0	All	All	All
Application	Gnu	Glibc	2.0.1	All	All	All
Application	Gnu	Glibc	2.0.2	All	All	All
Application	Gnu	Glibc	2.0.3	All	All	All
Application	Gnu	Glibc	2.0.4	All	All	All
Application	Gnu	Glibc	2.0.5	All	All	All
Application	Gnu	Glibc	2.0.6	All	All	All
Application	Gnu	Glibc	2.1	All	All	All
Application	Gnu	Glibc	2.1.1	All	All	All
Application	Gnu	Glibc	2.1.1.6	All	All	All
Application	Gnu	Glibc	2.1.2	All	All	All
Application	Gnu	Glibc	2.1.3	All	All	All
Application	Gnu	Glibc	2.1.9	All	All	All
Application	Gnu	Glibc	2.10.1	All	All	All
Application	Gnu	Glibc	2.11	All	All	All
Application	Gnu	Glibc	2.11.1	All	All	All
Application	Gnu	Glibc	2.11.2	All	All	All
Application	Gnu	Glibc	2.11.3	All	All	All
Application	Gnu	Glibc	2.12	All	All	All
Application	Gnu	Glibc	2.12.1	All	All	All
Application	Gnu	Glibc	2.12.2	All	All	All
Application	Gnu	Glibc	2.13	All	All	All
Application	Gnu	Glibc	2.14	All	All	All
Application	Gnu	Glibc	2.14.1	All	All	All

Application	Gnu	Glibc	2.15	All	All	All
Application	Gnu	Glibc	2.16	All	All	All
Application	Gnu	Glibc	2.17	All	All	All
Application	Gnu	Glibc	2.18	All	All	All
Application	Gnu	Glibc	All	All	All	All

References

Reference	Source
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Red Hat Customer Portal	MISC
Bug 1135841 – CVE-2014-6040 glibc: crash in code page decoding functions (IBM933, IBM935, IBM937, IBM939, IBM1364)	MISC
access.redhat.com | CVE-2014-6040	MISC
GNU glibc 'iconv()' Denial of Service Vulnerability	BID
Support / Security / Advisories / / MDVSA-2014:175 | Mandriva	MANDRIVA
sourceware.org Git - glibc.git/commitdiff	CONFIRM
Bug 17325 – iconv from ccsid 937 to utf-8 access invalid memory (CVE-2014-6040)	CONFIRM
GNU C Library: Multiple vulnerabilities (GLSA 201602-02) — Gentoo Security	GENTOO
sourceware.org Git - glibc.git/commitdiff	MISC
Debian -- Security Information -- DSA-3142-1 eglibc	DEBIAN
USN-2432-1: GNU C Library vulnerabilities | Ubuntu	UBUNTU
About Secunia Research | Flexera	SECUNIA
linux.oracle.com | ELSA-2015-0016	CONFIRM
oss-security - CVE request: glibc character set conversion from IBM code pages	MLIST
oss-security - Re: CVE request: glibc character set conversion from IBM code pages	MLIST
Security Advisory SA62146 - Oracle Linux update for glibc - Secunia	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 registred 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.

Free CVE JSON API cve.report/api

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