



CVE-2020-1751

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

Summary

CVE	CVE-2020-1751
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-17 19:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	An out-of-bounds write vulnerability was found in glibc before 2.31 when handling signal trampolines on PowerPC. Specific

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Gnu	Glibc	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link	T
1810719 – (CVE-2020-1751) CVE-2020-1751 glibc: array overflow in backtrace functions for powerpc	CONFIRM	bugzilla.redhat.com	Is
CVE-2020-1751 GNU C Library (glibc) Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	T
25423 – (CVE-2020-1751) Array overflow in backtrace on powerpc (CVE-2020-1751)	MISC	sourceware.org	Is
glibc: Multiple vulnerabilities (GLSA 202006-04) — Gentoo security	GENTOO	security.gentoo.org	
USN-4416-1: GNU C Library vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377356](#) Alibaba Cloud Linux Security Update for glibc (ALINUX3-SA-2022:0122)

[770068](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)

[900018](#) CBL-Mariner Linux Security Update for glibc 2.28

[903140](#) Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (2552)

[905968](#) Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (2552-1)

© [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](#)