



CVE-2019-7309

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-7309
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-03 02:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return z

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	All	All	All	All

References

Reference	Source	Link
24155 – (CVE-2019-7309) x32 memcmp can treat positive length as 0 (if sign bit in RDX is set) (CVE-2019-7309)	MISC	sourceware
GNU glibc CVE-2019-7309 Local Denial of Service Vulnerability	BID	www.securi
H.J. Lu - Re: [PATCH] x86-64 memcmp: Use unsigned Jcc instructions on size	MISC	sourceware
glibc: Multiple vulnerabilities (GLSA 202006-04) — Gentoo security	GENTOO	security.ger
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

900243 CBL-Mariner Linux Security Update for glibc 2.28

903380 Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (1940)

© [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](#)