



# CVE-2019-9169

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

## Summary

<b>CVE</b>	CVE-2019-9169
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-02-26 02:29:00 UTC
<b>Updated</b>	2023-11-07 03:13:00 UTC
<b>Description</b>	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer ove

## Risk And Classification

**Problem Types:** CWE-125

## 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>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Glibc</a>	All	All	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Web Gateway</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Steelstore Cloud Integrated Storage</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Steelstore Cloud Integrated Storage</a>	-	All	All	All

## References

### Reference

McAfee Security Bulletin - Web Gateway update fixes four third-party vulnerabilities (CVE-2018-18311, CVE-2018-5742, CVE-2019-9169, and

24114 – (CVE-2019-9169) regexec buffer read overrun in "grep -i '\(\\)\*.\*\\(\\)\*\\(\\)\*'"

March 2019 GNU C Vulnerabilities in NetApp Products | NetApp Product Security

[sourceware.org Git - glibc.git/commit](https://sourceware.org/Git-glibc.git/commit)

[Oracle Critical Patch Update Advisory - April 2022](#)

[support.f5.com/csp/article/K54823184](https://support.f5.com/csp/article/K54823184)

[sourceware.org Git - glibc.git/commit](https://sourceware.org/Git-glibc.git/commit)

[#34142 - AddressSanitizer reported heap-buffer-overflow - GNU bug report logs](#)

[glibc: Multiple vulnerabilities \(GLSA 202006-04\) — Gentoo security](#)

[USN-4416-1: GNU C Library vulnerabilities | Ubuntu security notices | Ubuntu](#)

[GNU glibc Stack Buffer Overflow and Heap Buffer Overflow Vulnerabilities](#)

[#34140 - AddressSanitizer reported heap-buffer-overflow when ignoring case - GNU bug report logs](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159188](#) Oracle Enterprise Linux Security Update for glibc (ELSA-2021-1585)

[159249](#) Oracle Enterprise Linux Security Update for glibc (ELSA-2021-9280)

[159295](#) Oracle Enterprise Linux Security Update for glibc (ELSA-2021-9344)

[239336](#) Red Hat Update for glibc (RHSA-2021:1585)

[352399](#) Amazon Linux Security Advisory for glibc: ALAS2-2021-1656

[591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

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

[902821](#) Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (1944)

[940275](#) AlmaLinux Security Update for glibc (ALSA-2021:1585)

[960868](#) Rocky Linux Security Update for glibc (RLSA-2021:1585)

© [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](#)