



CVE-2021-3999

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

Summary

CVE	CVE-2021-3999
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-24 16:15:00 UTC
Updated	2023-02-12 23:43:00 UTC
Description	A flaw was found in glibc. An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Netapp	E-series Performance Analyzer	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Nfs Plug-in	All	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
sourceware.org Git - glibc.git/commit	MISC	sourceware.org
CVE-2021-3999	MISC	security-tracker.debian.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
CVE-2021-3999 GNU C Library (glibc) Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
28769 – (CVE-2021-3999) Off-by-one buffer overflow/underflow in getcwd() (CVE-2021-3999)	MISC	sourceware.org
2024637 – (CVE-2021-3999) CVE-2021-3999 glibc: Off-by-one buffer overflow/underflow in getcwd()	MISC	bugzilla.redhat.com
[SECURITY] [DLA 3152-1] glibc security update	MLIST	lists.debian.org
oss-security - CVE-2021-3998 and CVE-2021-3999 in glibc's realpath() and getcwd()	MISC	www.openwall.com
sourceware.org Git - glibc.git/commit	MISC	sourceware.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159715](#) Oracle Enterprise Linux Security Update for glibc (ELSA-2022-0896)

[159720](#) Oracle Enterprise Linux Security Update for glibc (ELSA-2022-9234)

[181006](#) Debian Security Update for glibc (CVE-2021-3999)

[181138](#) Debian Security Update for glibc (DLA 3152-1)

[198685](#) Ubuntu Security Notification for GNU C Library Vulnerabilities (USN-5310-1)

[240148](#) Red Hat Update for glibc (RHSA-2022:0896)

[282318](#) Fedora Security Update for glibc (FEDORA-2022-918e18c52c)

[354097](#) Amazon Linux Security Advisory for glibc : ALAS2-2022-1857

[376419](#) Snap-Confine Local Privilege Escalation Vulnerability (Oh Snap! More Lemmings)

[376580](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) GNU C Library (glibc) Vulnerability (K24207649)

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

[671617](#) EulerOS Security Update for glibc (EulerOS-SA-2022-1565)

[671765](#) EulerOS Security Update for glibc (EulerOS-SA-2022-1823)

[671777](#) EulerOS Security Update for glibc (EulerOS-SA-2022-1827)

671777 EulerOS Security Update for glibc (EulerOS-SA-2022-1827)
671784 EulerOS Security Update for glibc (EulerOS-SA-2022-1840)
671815 EulerOS Security Update for glibc (EulerOS-SA-2022-1864)
672219 EulerOS Security Update for glibc (EulerOS-SA-2022-2608)
710605 Gentoo Linux GNU C Library Multiple Vulnerabilities (GLSA 202208-24)
751690 OpenSUSE Security Update for glibc (openSUSE-SU-2022:0330-1)
751712 SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2022:0441-1)
751867 SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2022:0832-1)
751910 SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2022:0909-1)
751983 SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2022:0330-1)
753208 SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2022:14923-1)
903758 Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (10699) (DEPRECATED)
904018 Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (10699-1)
940469 AlmaLinux Security Update for glibc (ALSA-2022:0896)
960118 Rocky Linux Security Update for glibc (RLSA-2022:896)
960854 Rocky Linux Security Update for glibc (RLSA-2022:0896)

© 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