



# CVE-2021-33574

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

## Summary

<b>CVE</b>	CVE-2021-33574
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-25 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:35:00 UTC
<b>Description</b>	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notifica

## Risk And Classification

### Problem Types: CWE-416

## 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	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Gnu	Glibc	2.32	All	All	All
Application	Gnu	Glibc	2.33	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All

Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller Firmware</a>	-	All	All	All

## References

Reference	Source	Link	Ta
[SECURITY] Fedora 34 Update: glibc-2.33-16.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 33 Update: glibc-2.32-8.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
27896 – mq_notify does not handle separately allocated thread attributes	MISC	<a href="https://sourceware.org">sourceware.org</a>	
glibc: Multiple vulnerabilities (GLSA 202107-07) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
[SECURITY] Fedora 33 Update: glibc-2.32-8.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
27896 – mq_notify does not handle separately allocated thread attributes	MISC	<a href="https://sourceware.org">sourceware.org</a>	
[SECURITY] [DLA 3152-1] glibc security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
[SECURITY] Fedora 34 Update: glibc-2.33-16.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE-2021-33574 GNU C Library (glibc) Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159493</a> Oracle Enterprise Linux Security Update for glibc (ELSA-2021-4358)
<a href="#">159561</a> Oracle Enterprise Linux Security Update for glibc (ELSA-2021-9560)
<a href="#">180332</a> Debian Security Update for glibc (CVE-2021-33574)
<a href="#">181138</a> Debian Security Update for glibc (DLA 3152-1)
<a href="#">239791</a> Red Hat Update for glibc security (RHSA-2021:4358)
<a href="#">281629</a> Fedora Security Update for glibc (FEDORA-2021-7ddb8b0537)
<a href="#">281689</a> Fedora Security Update for glibc (FEDORA-2021-f29b4643c7)
<a href="#">353127</a> Amazon Linux Security Advisory for glibc : ALAS2-2022-1736
<a href="#">591406</a> Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

<a href="#">670537</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2295)
<a href="#">670572</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2330)
<a href="#">670616</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2374)
<a href="#">670768</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2526)
<a href="#">670792</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2550)
<a href="#">670928</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2374)
<a href="#">670967</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2581)
<a href="#">710069</a> Gentoo Linux glibc Multiple vulnerabilities (GLSA 202107-07)
<a href="#">751195</a> SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2021:3290-1)
<a href="#">751196</a> SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2021:3289-1)
<a href="#">751200</a> OpenSUSE Security Update for glibc (openSUSE-SU-2021:3291-1)
<a href="#">751212</a> SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2021:3385-1)
<a href="#">751242</a> OpenSUSE Security Update for glibc (openSUSE-SU-2021:1374-1)
<a href="#">900034</a> CBL-Mariner Linux Security Update for glibc 2.28
<a href="#">902905</a> Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (4243)
<a href="#">940330</a> AlmaLinux Security Update for glibc (ALSA-2021:4358)

© [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](#)