



# CVE-2021-35942

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-35942
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-22 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:36:00 UTC
<b>Description</b>	The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (ir

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All

## References

Reference	Source	Link	Tag
Security Exceptions - glibc wiki	MISC	<a href="https://sourceware.org">sourceware.org</a>	
sourceware.org Git - glibc.git/commit	CONFIRM	<a href="https://sourceware.org">sourceware.org</a>	
sourceware.org Git - glibc.git/commit		<a href="https://sourceware.org">sourceware.org</a>	
CVE-2021-35942 GNU C Library (glibc) Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
28011 – (CVE-2021-35942) Wild read in wordexp (parse_param) (CVE-2021-35942)	CONFIRM	<a href="https://sourceware.org">sourceware.org</a>	
GNU C Library: Multiple Vulnerabilities (GLSA 202208-24) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	

[SECURITY] [DLA 3152-1] glibc security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can

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="#">179862</a> Debian Security Update for glibc (CVE-2021-35942)
<a href="#">181138</a> Debian Security Update for glibc (DLA 3152-1)
<a href="#">198685</a> Ubuntu Security Notification for GNU C Library Vulnerabilities (USN-5310-1)
<a href="#">239791</a> Red Hat Update for glibc security (RHSA-2021:4358)
<a href="#">281716</a> Fedora Security Update for glibc (FEDORA-2021-e14e86e40e)
<a href="#">281729</a> Fedora Security Update for glibc (FEDORA-2021-3f4132bb56)
<a href="#">352840</a> Amazon Linux Security Advisory for glibc: ALAS2-2021-1703
<a href="#">591406</a> Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
<a href="#">670703</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2461)
<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="#">670880</a> EulerOS Security Update for compat-glibc (EulerOS-SA-2021-2653)
<a href="#">671025</a> EulerOS Security Update for glibc (EulerOS-SA-2021-2660)
<a href="#">671239</a> EulerOS Security Update for compat-glibc (EulerOS-SA-2022-1158)
<a href="#">671255</a> EulerOS Security Update for glibc (EulerOS-SA-2022-1164)
<a href="#">710605</a> Gentoo Linux GNU C Library Multiple Vulnerabilities (GLSA 202208-24)
<a href="#">750897</a> SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2021:2480-1)
<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)

900060 CBL-Mariner Linux Security Update for glibc 2.28

903139 Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (4820)

940330 AlmaLinux Security Update for glibc (ALSA-2021:4358)

960043 Rocky Linux Security Update for glibc (RLSA-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](#)