



# CVE-2023-4813

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

## Summary

<b>CVE</b>	CVE-2023-4813
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-09-12 22:15:00 UTC
<b>Updated</b>	2023-11-10 18:15:00 UTC
<b>Description</b>	A flaw was found in glibc. In an uncommon situation, the gai_inet function may use memory that has been freed, resulting

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedora</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Glibc</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.8	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	9.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems Eus S390x</a>	9.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems S390x</a>	9.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	9.2_ppc64le	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	9.2_ppc64le	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	9.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.8	All	All	All

## References

Reference	Source	Link	Tags
CVE-2023-4813 GNU C Library (glibc) Vulnerability in NetApp Products   NetApp Product Security		<a href="https://security.netapp.com">security.netapp.com</a>	
cve-details	MISC	<a href="https://access.redhat.com">access.redhat.com</a>	

oss-security - Re: CVE-2023-4806, CVE-2023-5156: glibc: potential use-after-free in getaddrinfo()	MISC	<a href="http://www.openwall.com">www.openwall.com</a>	
2237798 – (CVE-2023-4813) CVE-2023-4813 glibc: potential use-after-free in gai_inet()	MISC	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>	
Red Hat	MISC	<a href="http://access.redhat.com">access.redhat.com</a>	
Red Hat	MISC	<a href="http://access.redhat.com">access.redhat.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">160965</a> Oracle Enterprise Linux Security Update for glibc (ELSA-2023-5455)
<a href="#">160968</a> Oracle Enterprise Linux Security Update for glibc (ELSA-2023-5453)
<a href="#">160973</a> Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12872)
<a href="#">160974</a> Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12873)
<a href="#">199987</a> Ubuntu Security Notification for GNU C Library Vulnerabilities (USN-6541-1)
<a href="#">242111</a> Red Hat Update for glibc (RHSA-2023:5453)
<a href="#">242118</a> Red Hat Update for glibc (RHSA-2023:5455)
<a href="#">242490</a> Red Hat Update for glibc (RHSA-2023:7409)
<a href="#">356310</a> Amazon Linux Security Advisory for glibc : ALAS2023-2023-359
<a href="#">378929</a> Alibaba Cloud Linux Security Update for glibc (ALINUX3-SA-2023:0124)
<a href="#">673448</a> EulerOS Security Update for glibc (EulerOS-SA-2024-1268)
<a href="#">673461</a> EulerOS Security Update for glibc (EulerOS-SA-2023-3212)
<a href="#">673463</a> EulerOS Security Update for glibc (EulerOS-SA-2024-1139)
<a href="#">673505</a> EulerOS Security Update for glibc (EulerOS-SA-2023-3269)
<a href="#">673617</a> EulerOS Security Update for glibc (EulerOS-SA-2023-3241)
<a href="#">673645</a> EulerOS Security Update for glibc (EulerOS-SA-2023-3330)
<a href="#">673703</a> EulerOS Security Update for glibc (EulerOS-SA-2023-3298)
<a href="#">673927</a> EulerOS Security Update for glibc (EulerOS-SA-2023-3177)
<a href="#">755072</a> SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2023:4047-1)
<a href="#">755110</a> SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2023:4110-1)

[941278](#) AlmaLinux Security Update for glibc (ALSA-2023:5455)

[941283](#) AlmaLinux Security Update for glibc (ALSA-2023:5453)

[961035](#) Rocky Linux Security Update for glibc (RLSA-2023:5455)

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)