CVE-2023-4813

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-4813
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-12 22:15:00 UTC
Updated	2023-11-10 18:15:00 UTC
Description	A flaw was found in glibc. In an uncommon situation, the gaih_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	Fedoraproject	Fedora	38	All	All	All
Application	Gnu	Glibc	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.8	All	All	All
Operating System	Redhat	Enterprise Linux Eus	9.2	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus S390x	9.2	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems S390x	9.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	9.2_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	9.2_ppc64le	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	9.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.8	All	All	All

References

Reference	Source	Link	Tags
CVE-2023-4813 GNU C Library (glibc) Vulnerability in NetApp Products | NetApp Product Security		security.netapp.com	
cve-details	MISC	access.redhat.com	

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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160965 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-5455)

160968 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-5453)

160973 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12872)

160974 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12873)

199987 Ubuntu Security Notification for GNU C Library Vulnerabilities (USN-6541-1)

242111 Red Hat Update for glibc (RHSA-2023:5453)

242118 Red Hat Update for glibc (RHSA-2023:5455)

242490 Red Hat Update for glibc (RHSA-2023:7409)

356310 Amazon Linux Security Advisory for glibc : ALAS2023-2023-359

378929 Alibaba Cloud Linux Security Update for glibc (ALINUX3-SA-2023:0124)

673448 EulerOS Security Update for glibc (EulerOS-SA-2024-1268)

673461 EulerOS Security Update for glibc (EulerOS-SA-2023-3212)

673463 EulerOS Security Update for glibc (EulerOS-SA-2024-1139)

673505 EulerOS Security Update for glibc (EulerOS-SA-2023-3269)

673617 EulerOS Security Update for glibc (EulerOS-SA-2023-3241)

673645 EulerOS Security Update for glibc (EulerOS-SA-2023-3330)

673703 EulerOS Security Update for glibc (EulerOS-SA-2023-3298)

673927 EulerOS Security Update for glibc (EulerOS-SA-2023-3177)

755072 SUSE Enterprise Linux Security Update for glibc (SUSE-SU-2023:4047-1)

755110 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)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**