GNU C Library Buffer Overflow Vulnerability

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

Summary

CVE	CVE-2023-4911
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-03 18:15:00 UTC
Updated	2024-01-03 15:15:00 UTC
Description	A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES env

Risk And Classification

EPSS: 0.673920000 probability, percentile 0.985750000 (date 2026-04-22)

CISA KEV: Listed on 2023-11-21; due 2023-12-12; ransomware use Unknown

Problem Types: CWE-787

CISA Known Exploited Vulnerability

Vendor	GNU
Product	GNU C Library
Name	GNU C Library Buffer Overflow Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status. For more information, please see: https://sourceware.org/git/?p=glibc.git;a=commitdiff;h=1056e5b4c3f2d90ed2b4a55f96add28da2f4c8fa, https://access.redhat.com/security/cve/cve-2023-4911, https://www.debian.org/security/2023/dsa-5514 ; https://nvd.nist.gov/vuln/detail/CVE-2023-4911

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Operating System	Fedoraproject	Fedora	39	All	All	All
Application	Gnu	Glibc	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Source	Link
oss-security - Re: CVE-2023-4911: Local Privilege Escalation in the glibc's ld.so	MISC	www.openwall.com
RHSA-2024:0033		access.redhat.com
oss-security - Re: CVE-2023-4911: Local Privilege Escalation in the glibc's ld.so	MISC	www.openwall.com
www.qualys.com/2023/10/03/cve-2023-4911/looney-tunables-local-privilege-esca...	MISC	www.qualys.com
oss-security - Re: linux-distros list membership application - CIQ Rocky Linux Security Team	MISC	www.openwall.com
CVE-2023-4911: Looney Tunables - Local Privilege Escalation in the glibc's ld.so | Qualys Security Blog	MISC	www.qualys.com
2238352 – (CVE-2023-4911) CVE-2023-4911 glibc: buffer overflow in ld.so leading to privilege escalation	MISC	bugzilla.redhat.com
[SECURITY] Fedora 39 Update: glibc-2.38-6.fc39 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.or
cve-details	MISC	access.redhat.com
CVE-2023-4911 GNU C Library (glibc) Vulnerability in NetApp Products | NetApp Product Security	MISC	security.netapp.com
Red Hat	MISC	access.redhat.com
packetstormsecurity.com/files/176288/Glibc-Tunables-Privilege-Escalation.html		packetstormsecurity
oss-security - Re: linux-distros list membership application - CIQ Rocky Linux Security Team	MISC	www.openwall.com
Red Hat	MISC	access.redhat.com
glibc ld.so Local Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity
oss-security - CVE-2023-4911: Local Privilege Escalation in the glibc's ld.so	MISC	www.openwall.com
Red Hat	MISC	access.redhat.com
glibc: Multiple vulnerabilities (GLSA 202310-03) — Gentoo security	MISC	security.gentoo.org
Red Hat	MISC	access.redhat.com
Full Disclosure: CVE-2023-4911: Local Privilege Escalation in the glibc's ld.so	MISC	seclists.org
oss-security - Re: linux-distros list membership application - CIQ Rocky Linux Security Team	MISC	www.openwall.com
[SECURITY] Fedora 37 Update: glibc-2.36-14.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.or
[SECURITY] Fedora 38 Update: glibc-2.37-10.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.or
Debian -- Security Information -- DSA-5514-1 glibc	MISC	www.debian.org
oss-security - Re: linux-distros list membership application - CIQ Rocky Linux Security Team	MISC	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160950 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12850)

160953 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12851)

160958 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12854)

160962 Oracle Enterprise Linux Security Update for glibc (ELSA-2023-12853)

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)

199798 Ubuntu Security Notification for GNU C Library Vulnerabilities (USN-6409-1)

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

242114 Red Hat Update for glibc (RHSA-2023:5454)

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

242120 Red Hat Update for glibc (RHSA-2023:5476)

284570 Fedora Security Update for glibc (FEDORA-2023-2b8c11ee75)

284571 Fedora Security Update for glibc (FEDORA-2023-028062484e)

285226 Fedora Security Update for glibc (FEDORA-2023-63e5a77522)

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

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

6000014 Debian Security Update for glibc (DSA 5514-1)

6140086 AWS Bottlerocket Security Update for glibc (GHSA-q944-5mwf-727h)

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

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

710764 Gentoo Linux glibc Multiple Vulnerabilities (GLSA 202310-03)

907418 Common Base Linux Mariner (CBL-Mariner) Security Update for glibc (31117-1)

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