

CVE-2023-4911

GNU C Library Buffer Overflow Vulnerability

CISA KEV since Nov 21, 2023

Actively exploited

Public exploit module (Metasploit)

A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.

EVRS

75/100

Urgent priority

CVSS V3.1

7.8

High · NVD

EPSS

0.638

99.22nd percentile · FIRST

CISA DEADLINE

Dec 12, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.638 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA note:** 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. a=commitdiff

h=1056e5b4c3f2d90ed2b4a55f96add28da2f4c8fa, <https://access.redhat.com/security/cve/cve-2023-4911>, <https://www.debian.org/security/2023/dsa-5514>

Basis: CISA KEV required action

Affected and fixed versions · 41 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
glibc	≥ 2.34 < 2.39	no fixed version listed	NVD
codeready linux builder	9.0	no fixed version listed	NVD
codeready linux builder eus	8.6 9.2 9.4 9.6	no fixed version listed	NVD
codeready linux builder for arm64	9.0 aarch64	no fixed version listed	NVD
codeready linux builder for arm64 eus	8.6 9.2 aarch64 9.4 aarch64 9.6 aarch64	no fixed version listed	NVD
codeready linux builder for ibm z systems	9.0 s390x	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
codeready linux builder for ibm z systems eus	8.6	no fixed version listed	NVD
	9.2 s390x		
	9.4 s390x		
	9.6 s390x		
codeready linux builder for power little endian	9.0 ppc64le	no fixed version listed	NVD

Sources

Vendor guidance	bugzilla.redhat.com/show_bug.cgi?id=2238352	Additional guidance	access.redhat.com/errata/RHSA-2023:5453
sourceware.org	sourceware.org/git/?p=glibc.git	NVD	nvd.nist.gov/vuln/detail/CVE-2023-4911
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-54750
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-4911		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.