LoongArch: BPF: Fix jump offset calculation in tailcall

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

Summary

CVE	CVE-2025-38723
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-04 16:15:42 UTC
Updated	2026-05-12 13:17:02 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Fix jump offset calculation in tailcall The

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 5dc615520c4dfb358245680f1904bad61116648e 1a782fa32e644aa9fbae6c8488f3e61221
CNA	Linux	Linux	affected 5dc615520c4dfb358245680f1904bad61116648e 17c010fe45def335fe03a0718935416b04
CNA	Linux	Linux	affected 5dc615520c4dfb358245680f1904bad61116648e f83d469e16bb1f75991ca67c56786fb2aa
CNA	Linux	Linux	affected 5dc615520c4dfb358245680f1904bad61116648e f2b5e50cc04d7a049b385bc1c93b9cbf5f
CNA	Linux	Linux	affected 5dc615520c4dfb358245680f1904bad61116648e 9262e3e04621558e875eb5afb5e726b64
CNA	Linux	Linux	affected 5dc615520c4dfb358245680f1904bad61116648e cd39d9e6b7e4c58fa77783e7aedf7ada51
CNA	Linux	Linux	affected 6.1
CNA	Linux	Linux	unaffected 6.1 semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.43 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.11 6.15.* semver
CNA	Linux	Linux	unaffected 6.16.2 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
git.kernel.org/stable/c/1a782fa32e644aa9fbae6c8488f3e61221ac96e1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/cd39d9e6b7e4c58fa77783e7aedf7ada51d02ea3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/9262e3e04621558e875eb5afb5e726b648cd5949	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/17c010fe45def335fe03a0718935416b04c7f349	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/f83d469e16bb1f75991ca67c56786fb2aaa42bea	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/f2b5e50cc04d7a049b385bc1c93b9cbf5f10c94f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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