ipv6: fix possible race in __fib6_drop_pcpu_from()

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

Summary

CVE	CVE-2024-40905
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 13:15:13 UTC
Updated	2026-05-12 12:16:59 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible race in __fib6_drop_pcpu_from() syzbot

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-476

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:H/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 d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected d52d3997f843ffefaa8d8462790ffcaca6c7419
CNA	Linux	Linux	affected 4.2
CNA	Linux	Linux	unaffected 4.2 semver
CNA	Linux	Linux	unaffected 5.4.279 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.95 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.35 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.6 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/09e5a5a80e205922151136069e440477d6816914	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/a0bc020592b54a8f3fa2b7f244b6e39e526c2e12	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/b01e1c030770ff3b4fe37fc7cc6bca03f594133f	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/2498960dac9b6fc49b6d1574f7cd1a4872744adf	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

git.kernel.org/stable/c/7e796c3fefa8b17b30e7252886ae8cffacd2b9ef	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/c693698787660c97950bc1f93a8dd19d8307153d	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.c
git.kernel.org/stable/c/c90af1cced2f669a7b2304584be4ada495eaa0e5	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.c
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.c
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.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.