xfrm6: check ip6_dst_idev() return value in xfrm6_get_saddr()

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

Summary

CVE	CVE-2024-40959
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 13:15:17 UTC
Updated	2026-05-12 12:17:00 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: xfrm6: check ip6_dst_idev() return value in xfrm6_get_sac

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: CWE-476

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 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321ca
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 semver
CNA	Linux	Linux	unaffected 4.19.317 4.19.* 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 6.1.96 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.36 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.7 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
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom

ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom

References

Reference	Source	Link
cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/600a62b4232ac027f788c3ca395bc2333adeaacf	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/c71761292d4d002a8eccb57b86792c4e3b3eb3c7	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/f897d7171652fcfc76d042bfec798b010ee89e41	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/9f30f1f1a51d91e19f5a09236bb0b59e6a07ad08	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/caf0bec84c62fb1cf6f7c9f0e8c857c87f8adbc3	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.co
git.kernel.org/stable/c/83c02fb2cc0afee5bb53cddf3f34f045f654ad6a	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.co
git.kernel.org/stable/c/20427b85781aca0ad072851f6907a3d4b2fed8d1	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/d46401052c2d5614da8efea5788532f0401cb164	af854a3a-2127-422b-91ae-364da2661108	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.