



# xfrm6: check ip6\_dst\_idev() return value in xfrm6\_get\_saddr()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-40959
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-07-12 13:15:17 UTC
<b>Updated</b>	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 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
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

## References

Reference	Source	Link
<a href="https://cert-portal.siemens.com/productcert/html/ssa-398330.html">cert-portal.siemens.com/productcert/html/ssa-398330.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-398330.html">cert-portal.siemens.co</a>
<a href="https://git.kernel.org/stable/c/600a62b4232ac027f788c3ca395bc2333adeaacf">git.kernel.org/stable/c/600a62b4232ac027f788c3ca395bc2333adeaacf</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/600a62b4232ac027f788c3ca395bc2333adeaacf">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/c71761292d4d002a8eccb57b86792c4e3b3eb3c7">git.kernel.org/stable/c/c71761292d4d002a8eccb57b86792c4e3b3eb3c7</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/c71761292d4d002a8eccb57b86792c4e3b3eb3c7">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/f897d7171652fcfc76d042bfec798b010ee89e41">git.kernel.org/stable/c/f897d7171652fcfc76d042bfec798b010ee89e41</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/f897d7171652fcfc76d042bfec798b010ee89e41">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/9f30f1f1a51d91e19f5a09236bb0b59e6a07ad08">git.kernel.org/stable/c/9f30f1f1a51d91e19f5a09236bb0b59e6a07ad08</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/9f30f1f1a51d91e19f5a09236bb0b59e6a07ad08">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/caf0bec84c62fb1cf6f7c9f0e8c857c87f8adbc3">git.kernel.org/stable/c/caf0bec84c62fb1cf6f7c9f0e8c857c87f8adbc3</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/caf0bec84c62fb1cf6f7c9f0e8c857c87f8adbc3">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.com/productcert/html/ssa-265688.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.co</a>
<a href="https://git.kernel.org/stable/c/83c02fb2cc0afee5bb53cddf3f34f045f654ad6a">git.kernel.org/stable/c/83c02fb2cc0afee5bb53cddf3f34f045f654ad6a</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/83c02fb2cc0afee5bb53cddf3f34f045f654ad6a">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-613116.html">cert-portal.siemens.com/productcert/html/ssa-613116.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-613116.html">cert-portal.siemens.co</a>
<a href="https://git.kernel.org/stable/c/20427b85781aca0ad072851f6907a3d4b2fed8d1">git.kernel.org/stable/c/20427b85781aca0ad072851f6907a3d4b2fed8d1</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/20427b85781aca0ad072851f6907a3d4b2fed8d1">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-355557.html">cert-portal.siemens.com/productcert/html/ssa-355557.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-355557.html">cert-portal.siemens.co</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/01/msg00001.html">lists.debian.org/debian-lts-announce/2025/01/msg00001.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2025/01/msg00001.html">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/d46401052c2d5614da8efea5788532f0401cb164">git.kernel.org/stable/c/d46401052c2d5614da8efea5788532f0401cb164</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/d46401052c2d5614da8efea5788532f0401cb164">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)