



# net: fix data-races around sk->sk\_forward\_alloc

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

## Summary

<b>CVE</b>	CVE-2024-53124
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-12-02 14:15:13 UTC
<b>Updated</b>	2026-05-12 13:16:22 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: net: fix data-races around sk->sk_forward_alloc Syzkaller

## 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

**EPSS:** 0.000140000 probability, percentile 0.026520000 (date 2026-05-12)

**Problem Types:** CWE-362

## 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
Operating System	Linux	Linux Kernel	6.12	rc1	All	All
Operating System	Linux	Linux Kernel	6.12	rc2	All	All
Operating System	Linux	Linux Kernel	6.12	rc3	All	All
Operating System	Linux	Linux Kernel	6.12	rc4	All	All
Operating System	Linux	Linux Kernel	6.12	rc5	All	All
Operating System	Linux	Linux Kernel	6.12	rc6	All	All
Operating System	Linux	Linux Kernel	6.12	rc7	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 695fb0b
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 fe2c0bd
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 c3d052c
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 be7c61e
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 3f51f8c
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 d285eb
CNA	Linux	Linux	affected e994b2f0fb9229aeff5eea9541320bd7b2ca8714 073d89
CNA	Linux	Linux	affected 4.4
CNA	Linux	Linux	unaffected 4.4 semver
CNA	Linux	Linux	unaffected 5.4.290 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.234 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.177 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.127 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.74 6.6.* semver
CNA	Linux	Linux	unaffected 6.11.10 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - BIOS	affected * 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 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	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://cert-portal.siemens.com/productcert/html/ssa-503939.html">cert-portal.siemens.com/productcert/html/ssa-503939.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-503939.html">cert-portal.siemens.co</a>
<a href="https://git.kernel.org/stable/c/c3d052cae566ec2285f5999958a5deb415a0f59e">git.kernel.org/stable/c/c3d052cae566ec2285f5999958a5deb415a0f59e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/c3d052cae566ec2285f5999958a5deb415a0f59e">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/073d89808c065ac4c672c0a613a71b27a80691cb">git.kernel.org/stable/c/073d89808c065ac4c672c0a613a71b27a80691cb</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/073d89808c065ac4c672c0a613a71b27a80691cb">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/03/msg00002.html">lists.debian.org/debian-lts-announce/2025/03/msg00002.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2025/03/msg00002.html">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/be7c61ea5f816168c38955eb4e898adc8b4b32fd">git.kernel.org/stable/c/be7c61ea5f816168c38955eb4e898adc8b4b32fd</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/be7c61ea5f816168c38955eb4e898adc8b4b32fd">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/3f51f8c9d28954cf380100883a02eed35a8277e9">git.kernel.org/stable/c/3f51f8c9d28954cf380100883a02eed35a8277e9</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/3f51f8c9d28954cf380100883a02eed35a8277e9">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/d285eb9d0641c8344f2836081b4ccb7b3c5cc1b6">git.kernel.org/stable/c/d285eb9d0641c8344f2836081b4ccb7b3c5cc1b6</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/d285eb9d0641c8344f2836081b4ccb7b3c5cc1b6">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/03/msg00001.html">lists.debian.org/debian-lts-announce/2025/03/msg00001.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2025/03/msg00001.html">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/695fb0b9aecfd5dd5b2946ba8897ac2c1eef654d">git.kernel.org/stable/c/695fb0b9aecfd5dd5b2946ba8897ac2c1eef654d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/695fb0b9aecfd5dd5b2946ba8897ac2c1eef654d">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/fe2c0bd6d1e29ccefdc978b9a290571c93c27473">git.kernel.org/stable/c/fe2c0bd6d1e29ccefdc978b9a290571c93c27473</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/fe2c0bd6d1e29ccefdc978b9a290571c93c27473">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)