



# netfilter: ipset: Fix suspicious rcu\_dereference\_protected()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-40993
<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 13:15:20 UTC
<b>Updated</b>	2026-05-12 12:17:01 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: Fix suspicious rcu\_dereference\_protected()

## 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

**EPSS:** 0.000270000 probability, percentile 0.077810000 (date 2026-05-12)

**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

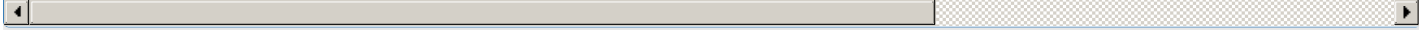


### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.1.95	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.10	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.6.35	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	6.9.6	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected c0761d1f1ce1d5b85b5e82bbb714df12de1aa8c3 3799d0
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 93b53c202b51a69e42ca57f5a183f7e008e19f83 72d961
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 0f1bb77c6d837c9513943bc7c08f04c5cc5c6568 523bed
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 390b353d1a1da3e9c6c0fd14fe650d69063c95d6 788d5f
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 2ba35b37f780c6410bb4bba9c3072596d8576702 94dd4
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 90ae20d47de602198eb69e6cd7a3db3420abfc08 3fc09e
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 4e7aaa6b82d63e8ddcbfb56b4fd3d014ca586f10 8ecd06
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.1.95 6.1.96 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.6.35 6.6.36 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 6.9.6 6.9.7 semver
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem</a>	affected * custom



### References

Reference	Source	Link
<a href="https://git.kernel.org/stable/c/94dd411c18d7fff9e411555d5c662d29416501e4">git.kernel.org/stable/c/94dd411c18d7fff9e411555d5c662d29416501e4</a>	<a href="https://git.kernel.org/stable/c/94dd411c18d7fff9e411555d5c662d29416501e4">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/8ecd06277a7664f4ef018abae3abd3451d64e7a6">git.kernel.org/stable/c/8ecd06277a7664f4ef018abae3abd3451d64e7a6</a>	<a href="https://git.kernel.org/stable/c/8ecd06277a7664f4ef018abae3abd3451d64e7a6">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/72d9611968867cc4c5509e7708b1507d692b797a">git.kernel.org/stable/c/72d9611968867cc4c5509e7708b1507d692b797a</a>	<a href="https://git.kernel.org/stable/c/72d9611968867cc4c5509e7708b1507d692b797a">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">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>	<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">0b142b55-0307-4c5a-b3c9-f314f3fb7c5e</a>	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="https://git.kernel.org/stable/c/3fc09e1ca854bc234e007a56e0f7431f5e2defb5">git.kernel.org/stable/c/3fc09e1ca854bc234e007a56e0f7431f5e2defb5</a>	<a href="https://git.kernel.org/stable/c/3fc09e1ca854bc234e007a56e0f7431f5e2defb5">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/788d585e62f487bc4536d454937f737b70d39a33">git.kernel.org/stable/c/788d585e62f487bc4536d454937f737b70d39a33</a>	<a href="https://git.kernel.org/stable/c/788d585e62f487bc4536d454937f737b70d39a33">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/3799d02ae4208af08e81310770d8754863a246a1">git.kernel.org/stable/c/3799d02ae4208af08e81310770d8754863a246a1</a>	<a href="https://git.kernel.org/stable/c/3799d02ae4208af08e81310770d8754863a246a1">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/523bed6489e089dd8040e72453fb79da47b144c2">git.kernel.org/stable/c/523bed6489e089dd8040e72453fb79da47b144c2</a>	<a href="https://git.kernel.org/stable/c/523bed6489e089dd8040e72453fb79da47b144c2">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://git.kernel.org">git.kernel.org</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>	<a href="https://lists.debian.org/debian-lts-announce/2025/01/msg00001.html">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="https://lists.debian.org">lists.debian.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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)