



pps: Fix a use-after-free

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

Summary

CVE	CVE-2024-57979
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-02-27 02:15:11 UTC
Updated	2026-05-12 13:16:25 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: pps: Fix a use-after-free On a board running ntpd and gps

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

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

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 d953e0e837e65ecc1ddaa4f9560f7925878a0de6 785c7f
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 1a773f
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 c4041k
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 91932c
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 cd3bbc
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 7e5ee6
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 85241f
CNA	Linux	Linux	affected d953e0e837e65ecc1ddaa4f9560f7925878a0de6 c79a39
CNA	Linux	Linux	affected 77327a71f9841b7dfa708195d1cb133d4ef4a989 git
CNA	Linux	Linux	affected cd59fb14918a6b20c1ac8be121fa6397b97b00cb git
CNA	Linux	Linux	affected 49626fbb0360332e40fd76a48cb2ba876d6134ad git
CNA	Linux	Linux	affected 3.9
CNA	Linux	Linux	unaffected 3.9 semver
CNA	Linux	Linux	unaffected 5.4.291 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.235 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.179 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.129 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.76 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.13 6.12.* semver
CNA	Linux	Linux	unaffected 6.13.2 6.13.* semver
CNA	Linux	Linux	unaffected 6.14 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/05/msg00030.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org

git.kernel.org/stable/c/785c78ed0d39d1717cca3ef931d3e51337b5e90e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/c4041b6b0a7a3def8cf3f3d6120ff337bc4c40f7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/85241f7de216f8298f6e48540ea13d7dcd100870	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/1a7735ab2cb9747518a7416fb5929e85442dec62	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/7e5ee3281dc09014367f5112b6d566ba36ea2d49	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com
git.kernel.org/stable/c/cd3bbcb6b3a7caa5ce67de76723b6d8531fb7f64	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/91932db1d96b2952299ce30c1c693d834d10ace6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/03/msg00028.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/c79a39dc8d060b9e64e8b0fa9d245d44befeefbe	416baaa9-dc9f-4396-8d5f-8c081fb06d67	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.

© [CVE.report](https://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/cve). 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