



net: openvswitch: Fix Use-After-Free in ovs_ct_exit

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2024-27395
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-14 15:12:27 UTC
Updated	2026-05-12 12:16:32 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: Fix Use-After-Free in ovs_ct_exit Since

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-416

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 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 11efd5cb04a184eea4f57b68ea63ddd4631f
CNA	Linux	Linux	affected 4.18
CNA	Linux	Linux	unaffected 4.18 semver
CNA	Linux	Linux	unaffected 4.19.313 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.275 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.216 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.158 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.90 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.30 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.9 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 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	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/5ea7b72d4fac2fdb0425cd8f2ea33abe95235b2	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/edee0758747d7c219e29db9ed1d4eb33e8d32865	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.cc
git.kernel.org/stable/c/9048616553c65e750d43846f225843ed745ec0d4	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org

git.kernel.org/stable/c/35880c3fa6f8fe281a19975d2992644588ca33d3	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/ea5e164a2110d2fb9e16c8a29e4501882235137	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/bca6fa2d9a9f560e6b89fd5190b05cc2f5d422c1	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.com
git.kernel.org/stable/c/2db9a8c0a01fa1c762c1e61a13c212c492752994	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00020.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/589523cf0b384164e445dd5db8d5b1bf97982424	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.

© [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