



tcp: Use refcount_inc_not_zero() in tcp_twsk_unique().

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

Summary

CVE	CVE-2024-36904
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-30 16:15:13 UTC
Updated	2026-05-12 12:16:49 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: tcp: Use refcount_inc_not_zero() in tcp_twsk_unique(). Ar

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 ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected ec94c2696f0bcd5ae92a553244e4ac30d217
CNA	Linux	Linux	affected 4.16
CNA	Linux	Linux	unaffected 4.16 semver
CNA	Linux	Linux	unaffected 4.19.314 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.276 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.217 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.159 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.91 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.31 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.10 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
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
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom

References

Reference	Source	Link
-----------	--------	------

cert-portal.siemens.com/productcert/html/ssa-398330.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/517e32ea0a8c72202d0d8aa8df50a7cd3d6fdefc	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
security.netapp.com/advisory/ntap-20240905-0004	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com
git.kernel.org/stable/c/6e48faad92be13166184d21506e4e54c79c13adc	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.co
git.kernel.org/stable/c/84546cc1aeeb4df3e444b18a4293c9823f974be9	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/1d9cf07810c30ef7948879567d10fd1f01121d34	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/1796ca9c6f5bd50554214053af5f47d112818ee3	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00019.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/13ed7cdf079686ccd3618335205700c03f6fb446	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/27b0284d8be182a81feb65581ab6a724dfd596e8	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/f2db7230f73a80dbb179deab78f88a7947f0ab7e	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 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](#)