tcp: defer shutdown(SEND_SHUTDOWN) for TCP_SYN_RECV sockets

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-36905
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-30 16:15:14 UTC
Updated	2026-05-12 12:16:49 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: tcp: defer shutdown(SEND_SHUTDOWN) for TCP_SYN_

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

Problem Types: CWE-369

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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321c
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 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	Linux	Linux Kernel	affected 1da177e4c3f4 34e41a031fd7 custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f4 ed5e279b69e0 custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f4 413c33b9f3bc custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f 2552c9d9440f custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f4 3fe4ef0568a4 custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f4 f47d0d32fa94 custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f4 cbf232ba11bc custom
ADP	Linux	Linux Kernel	affected 1da177e4c3f4 94062790aedb custom
ADP	Linux	Linux Kernel	unaffected 4.19.314 4.20 custom
ADP	Linux	Linux Kernel	unaffected 5.10.217 5.11 custom
ADP	Linux	Linux Kernel	unaffected 5.15.159 5.16 custom

ADP	Linux	Linux Kernel	unaffected 6.1.91 6.2 custom
ADP	Linux	Linux Kernel	unaffected 6.6.31 6.7 custom
ADP	Linux	Linux Kernel	unaffected 6.9
ADP	Linux	Linux Kernel	unaffected 2.6.12 custom
ADP	Linux	Linux Kernel	affected 2.6.12
ADP	Linux	Linux Kernel	unaffected 5.4.276 5.5 custom
ADP	Linux	Linux Kernel	unaffected 6.8.10 6.9 custom
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
www.openwall.com/lists/oss-security/2024/11/12/4	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.openwall.com
www.openwall.com/lists/oss-security/2024/10/29/1	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
www.openwall.com/lists/oss-security/2024/11/12/5	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
git.kernel.org/stable/c/3fe4ef0568a48369b1891395d13ac593b1ba41b1	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
www.openwall.com/lists/oss-security/2024/11/12/4	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
git.kernel.org/stable/c/f47d0d32fa94e815fdd78b8b88684873e67939f4	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/94062790aedb505bdda209b10bea47b294d6394f	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
www.openwall.com/lists/oss-security/2024/11/12/6	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
git.kernel.org/stable/c/2552c9d9440f8e7a2ed0660911ff00f25b90a0a4	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
www.openwall.com/lists/oss-security/2024/10/29/1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	www.openwall.com
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
www.openwall.com/lists/oss-security/2024/10/30/1	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
access.redhat.com/security/cve/cve-2024-36905	134c704f-9b21-4f2e-91b3-4a467353bcc0	access.redhat.com
git.kernel.org/stable/c/ed5e279b69e007ce6c0fe82a5a534c1b19783214	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/cbf232ba11bc86a5281b4f00e1151349ef4d45cf	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/413c33b9f3bc36fdf719690a78824db9f88a9485	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
security.netapp.com/advisory/ntap-20240905-0005	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com
git.kernel.org/stable/c/34e41a031fd7523bf1cd00a2adca2370aebea270	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
alas.aws.amazon.com/cve/html/CVE-2024-36905.html	134c704f-9b21-4f2e-91b3-4a467353bcc0	alas.aws.amazon.com
github.com/cisagov/vulnrichment/issues/130	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
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.