



net: relax socket state check at accept time.

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

Summary

CVE	CVE-2024-36484
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-06-21 11:15:10 UTC
Updated	2026-05-12 12:16:48 UTC

Description In the Linux kernel, the following vulnerability has been resolved: net: relax socket state check at accept time. Christoph rep

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: 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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 34e41a031fd7523bf1cd00a2adca2370aebec
CNA	Linux	Linux	affected ed5e279b69e007ce6c0fe82a5a534c1b1978
CNA	Linux	Linux	affected 413c33b9f3bc36fdf719690a78824db9f88a94
CNA	Linux	Linux	affected 2552c9d9440f8e7a2ed0660911ff00f25b90a0
CNA	Linux	Linux	affected 3fe4ef0568a48369b1891395d13ac593b1ba4
CNA	Linux	Linux	affected f47d0d32fa94e815fdd78b8b88684873e6793
CNA	Linux	Linux	affected 94062790aedb505bdda209b10bea47b294d0
CNA	Linux	Linux	affected 94062790aedb505bdda209b10bea47b294d0
CNA	Linux	Linux	affected cbf232ba11bc86a5281b4f00e1151349ef4d4
CNA	Linux	Linux	affected 6.9
CNA	Linux	Linux	unaffected 6.9 semver
CNA	Linux	Linux	unaffected 4.19.319 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.281 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.223 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.164 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.93 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.33 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.4 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * 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	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * 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

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/59801e88c99f7c3f44a4d20af6ba6417aa359b5d	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/5f9a04a94fd1894d7009055ab8e5832a0242dba3	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/7de00adc9bd035d861ba4177848ca0bfa5ed1e04	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/c09ddc605893df542c6cf8dde6a57a93f7cf0adb	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/21c14c556cccd0cb54b71ec5e901e64ba84c7165	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.co
git.kernel.org/stable/c/26afda78cda3da974fd4c287962c169e9462c495	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/87bdc9f6f58b4417362d6932b49b828e319f97dc	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/6e03006548c66b979f4e5e9fc797aac4dad82822	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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report