



block/ioctl: prefer different overflow check

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

Summary

CVE	CVE-2024-41000
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-12 13:15:20 UTC
Updated	2026-05-12 12:17:02 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: block/ioctl: prefer different overflow check Running syzkall

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-190

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	Debian	Debian Linux	11.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 8f6dfa1f1efe6dcca2d43e575491d8fcbe922ff
CNA	Linux	Linux	affected 5010c27120962c85d2f421d2cf211791c9603
CNA	Linux	Linux	affected ef31cc87794731ffcb578a195a2c47d744e25f
CNA	Linux	Linux	affected cb16cc1abda18a9514106d2ac8c8d7abc0be
CNA	Linux	Linux	affected 6f64f866aa1ae6975c95d805ed51d7e9433a0
CNA	Linux	Linux	affected 6f64f866aa1ae6975c95d805ed51d7e9433a0
CNA	Linux	Linux	affected bcdc288e7bc008daf38ef0401b53e4a8bb61b
CNA	Linux	Linux	affected 6.8
CNA	Linux	Linux	unaffected 6.8 semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.96 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.36 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.7 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

References

Reference	Source	Link
git.kernel.org/stable/c/61ec76ec930709b7bcd69029ef1fe90491f20cf9	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/ccb326b5f9e623eb7f130fbf2505ec0e2dcaff9	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/3220c90f4dbdc6d20d0608b164d964434a810d66	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/54160fb1db2de367485f21e30196c42f7ee0be4e	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/fd841ee01fb4a79cb7f5cc424b5c96c3a73b2d1e	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
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/58706e482bf45c4db48b0c53aba2468c97adda24	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