xsk: validate user input for XDP_{UMEM|COMPLETION}_FILL_RING

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

Summary

CVE	CVE-2024-35976
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-20 10:15:12 UTC
Updated	2026-05-12 12:16:44 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: xsk: validate user input for XDP_{UMEM|COMPLETION}_

Risk And Classification

Primary CVSS: v3.1 6.7 MEDIUM from ADP

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

Problem Types: CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

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 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 423f38329d267969130fb6f2c685f73d726875
CNA	Linux	Linux	affected 4.18
CNA	Linux	Linux	unaffected 4.18 semver
CNA	Linux	Linux	unaffected 4.19.317 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.278 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.216 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.156 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.87 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.28 6.6.* semver
CNA	Linux	Linux	unaffected 6.8.7 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Linux	Linux Kernel	affected 4.18
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
git.kernel.org/stable/c/beb99266830520e15fbc6ca8cc5a5240d76851fd	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.co
git.kernel.org/stable/c/a82984b3c6a7e8c7937dba6e857ddf829d149417	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/2a523f14a3f53b46ff0e1fafd215b0bc5f6783aa	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/237f3cf13b20db183d3706d997eedc3c49eacd44	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/f0a068de65d5b7358e9aff792716afa9333f3922	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/0b45c25d60e38f5c2cb6823f886773a34323306d	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/2eb979fbb2479bcd7e049f2f9978b6590dd8a0e6	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/b143e19dc28c3211f050f7848d87d9b0a170e10c	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 registred 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**