



media: pvrusb2: fix uaf in pvr2_context_set_notify

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

Summary

CVE	CVE-2024-26875
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-17 11:15:09 UTC
Updated	2026-05-12 12:16:22 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: media: pvrusb2: fix uaf in pvr2_context_set_notify [Syzbot

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from ADP

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

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:H/PR:H/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 e5be15c63804e05b5a94197524023702a259e308 ed80
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 d29e
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 ab89
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 eb6e
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 3a1e
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 8e60
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 40cd
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 eaa4
CNA	Linux	Linux	affected e5be15c63804e05b5a94197524023702a259e308 0a0b
CNA	Linux	Linux	affected 2.6.26
CNA	Linux	Linux	unaffected 2.6.26 semver
CNA	Linux	Linux	unaffected 4.19.311 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.273 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.214 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.153 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.83 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.23 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.11 6.7.* semver
CNA	Linux	Linux	unaffected 6.8.2 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Linux	Linux Kernel	affected e5be15c63804 ed8000e1e8e9 custom
ADP	Linux	Linux Kernel	affected e5be15c63804 d29ed08964ce custom
ADP	Linux	Linux Kernel	affected e5be15c63804 ab896d93fd6a custom
ADP	Linux	Linux Kernel	affected e5be15c63804 eb6e9dce979c custom
ADP	Linux	Linux Kernel	affected e5be15c63804 3a1ec89708d2 custom
ADP	Linux	Linux Kernel	affected e5be15c63804 8e60b99f6b7c custom

ADP	Linux	Linux Kernel	affected e5be15c63804 40cd818fae87 custom
ADP	Linux	Linux Kernel	affected e5be15c63804 eaa410e05bdf custom
ADP	Linux	Linux Kernel	affected e5be15c63804 0a0b79ea55de custom
ADP	Linux	Linux Kernel	affected 2.6.26
ADP	Linux	Linux Kernel	unaffected 2.6.26 custom
ADP	Linux	Linux Kernel	unaffected 4.19.311 4.20 custom
ADP	Linux	Linux Kernel	unaffected 5.4.273 5.5 custom
ADP	Linux	Linux Kernel	unaffected 5.10.214 5.11 custom
ADP	Linux	Linux Kernel	unaffected 5.15.153 5.16 custom
ADP	Linux	Linux Kernel	unaffected 6.183 6.2 custom
ADP	Linux	Linux Kernel	unaffected 6.6.23 6.7 custom
ADP	Linux	Linux Kernel	unaffected 6.7.11 6.8 custom
ADP	Linux	Linux Kernel	unaffected 6.8.2 6.9 custom
ADP	Linux	Linux Kernel	unaffected 6.9 * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/0a0b79ea55de8514e1750884e5fec77f9fdd01ee	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/8e60b99f6b7ccb3badeb512f5eb613ad45904592	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.com
git.kernel.org/stable/c/3a1ec89708d2e57e2712f46241282961b1a7a475	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/eaa410e05bdf562c90b23cdf2d9327f9c4625e16	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/40cd818fae875c424a8335009db33c7b5a07de3a	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/d29ed08964cec8b9729bc55c7bb23f679d7a18fb	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/ed8000e1e8e9684ab6c30cf2b526c0cea039929c	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/ab896d93fd6a2cd1afeb034c3cc9226cb499209f	af854a3a-2127-422b-91ae-364da2661108	git.kernel.org
git.kernel.org/stable/c/eb6e9dce979c08210ff7249e5e0eceb8991bfcd7	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 OID mappings associated with 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](#)