



# HID: roccat: fix use-after-free in roccat\_report\_event

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-43111
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 10:16:24 UTC
<b>Updated</b>	2026-05-08 19:45:15 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: HID: roccat: fix use-after-free in roccat_report_event rocca

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

**EPSS:** 0.000130000 probability, percentile 0.023990000 (date 2026-05-12)

**Problem Types:** CWE-416

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

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	Linux	Linux Kernel	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 206f5f2fcb5ff5bb0c60f9e9189937f3ca03e378 e6a445513fbc6a0329d2d5ff375b6725750ec5a6 git
CNA	Linux	Linux	affected 206f5f2fcb5ff5bb0c60f9e9189937f3ca03e378 e16a6d11bd77b81632165f02cf0d5946df74b3b7 git
CNA	Linux	Linux	affected 206f5f2fcb5ff5bb0c60f9e9189937f3ca03e378 36bb2d0b915014bbdc5044982b31b57b78045b93 git
CNA	Linux	Linux	affected 206f5f2fcb5ff5bb0c60f9e9189937f3ca03e378 bca0b595e15450dd66b1153c76c4ef1087ee011b git
CNA	Linux	Linux	affected 206f5f2fcb5ff5bb0c60f9e9189937f3ca03e378 d802d848308b35220f21a8025352f0c0aba15c12 git
CNA	Linux	Linux	affected 2.6.35
CNA	Linux	Linux	unaffected 2.6.35 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/e6a445513fbc6a0329d2d5ff375b6725750ec5a6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/e6a445513fbc6a0329d2d5ff375b6725750ec5a6">git.kernel.org</a>	Patch
git.kernel.org/stable/c/d802d848308b35220f21a8025352f0c0aba15c12	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/d802d848308b35220f21a8025352f0c0aba15c12">git.kernel.org</a>	Patch
git.kernel.org/stable/c/bca0b595e15450dd66b1153c76c4ef1087ee011b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/bca0b595e15450dd66b1153c76c4ef1087ee011b">git.kernel.org</a>	Patch
git.kernel.org/stable/c/e16a6d11bd77b81632165f02cf0d5946df74b3b7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/e16a6d11bd77b81632165f02cf0d5946df74b3b7">git.kernel.org</a>	Patch
git.kernel.org/stable/c/36bb2d0b915014bbdc5044982b31b57b78045b93	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/36bb2d0b915014bbdc5044982b31b57b78045b93">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

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](#) 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](#)