accel/qaic: Handle DBC deactivation if the owner went away

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

Summary

CVE	CVE-2026-43007
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 15:16:44 UTC
Updated	2026-05-07 20:24:32 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: accel/qaic: Handle DBC deactivation if the owner went aw

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

EPSS: 0.000180000 probability, percentile 0.048290000 (date 2026-05-05)

Problem Types: CWE-415

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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 129776ac2e38231fa9c02ce20e116c99de291666 2dd67966f39a2abf8ccb4865031c722e40e01b7f git
CNA	Linux	Linux	affected 129776ac2e38231fa9c02ce20e116c99de291666 08021f2d4a557d6491e3bcc288e96425f50aa3cf git
CNA	Linux	Linux	affected 129776ac2e38231fa9c02ce20e116c99de291666 f403094d9075d7c565a3d81002b781c325cb3c07 gi
CNA	Linux	Linux	affected 129776ac2e38231fa9c02ce20e116c99de291666 ee0180e77e6c8482644569632065411de844c515 g
CNA	Linux	Linux	affected 129776ac2e38231fa9c02ce20e116c99de291666 2feec5ae5df785658924ab6bd91280dc3926507c git
CNA	Linux	Linux	affected 6.4
CNA	Linux	Linux	unaffected 6.4 semver
CNA	Linux	Linux	unaffected 6.6.134 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.81 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.22 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.12 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ee0180e77e6c8482644569632065411de844c515	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2feec5ae5df785658924ab6bd91280dc3926507c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/08021f2d4a557d6491e3bcc288e96425f50aa3cf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f403094d9075d7c565a3d81002b781c325cb3c07	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2dd67966f39a2abf8ccb4865031c722e40e01b7f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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