bcache: fix cached_dev.sb_bio use-after-free and crash

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

Summary

CVE	CVE-2026-31580
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:32 UTC
Updated	2026-04-27 20:29:15 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: bcache: fix cached_dev.sb_bio use-after-free and crash Ir

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 0.048130000 (date 2026-04-27)

Problem Types: CWE-416

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 cafe563591446cf80bfbc2fe3bc72a2e36cf1060 47fa09fe7f3e09df28a51cb2cbd8f5d2f7f6edc1 git
CNA	Linux	Linux	affected cafe563591446cf80bfbc2fe3bc72a2e36cf1060 add4982510f3b7c318a2dd7438bdc9c63171e753 git
CNA	Linux	Linux	affected cafe563591446cf80bfbc2fe3bc72a2e36cf1060 2d6965581e164fa2ba3f7652ddae5535f6336576 git
CNA	Linux	Linux	affected cafe563591446cf80bfbc2fe3bc72a2e36cf1060 4f71c8ba2dc009042493021d94a9718fbe2ebf27 git
CNA	Linux	Linux	affected cafe563591446cf80bfbc2fe3bc72a2e36cf1060 383f7fec0de8cee1cf7ae1f9d9f14044a61f10f9 git
CNA	Linux	Linux	affected cafe563591446cf80bfbc2fe3bc72a2e36cf1060 fec114a98b8735ee89c75216c45a78e28be0f128 git
CNA	Linux	Linux	affected 3.10
CNA	Linux	Linux	unaffected 3.10 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 7.0.1 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/47fa09fe7f3e09df28a51cb2cbd8f5d2f7f6edc1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/383f7fec0de8cee1cf7ae1f9d9f14044a61f10f9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/fec114a98b8735ee89c75216c45a78e28be0f128	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/add4982510f3b7c318a2dd7438bdc9c63171e753	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2d6965581e164fa2ba3f7652ddae5535f6336576	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/4f71c8ba2dc009042493021d94a9718fbe2ebf27	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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

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

Free CVE JSON API cve.report/api

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