



# x86/cpu: Remove X86\_CR4\_FRED from the CR4 pinned bits mask

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-31561
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-24 15:16:30 UTC
<b>Updated</b>	2026-04-27 20:30:14 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: x86/cpu: Remove X86\_CR4\_FRED from the CR4 pinned

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000180000 probability, percentile 0.046080000 (date 2026-04-27)

**Problem Types:** NVD-CWE-noinfo

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 ff45746bf005f96e42bea466698e3fdbf926013 d7853d9fe94abf43b46c57b0b7f8418198b7615a git
CNA	Linux	Linux	affected ff45746bf005f96e42bea466698e3fdbf926013 a6e14114684d2324e5401617d6d01acb4a4e0e22 git
CNA	Linux	Linux	affected ff45746bf005f96e42bea466698e3fdbf926013 00d956dafa76f86a73424fe5cce3d604a8be2e4b git
CNA	Linux	Linux	affected ff45746bf005f96e42bea466698e3fdbf926013 411df123c017169922cc767affce76282b8e6c85 git
CNA	Linux	Linux	affected 6.9
CNA	Linux	Linux	unaffected 6.9 semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/411df123c017169922cc767affce76282b8e6c85	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/a6e14114684d2324e5401617d6d01acb4a4e0e22	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/d7853d9fe94abf43b46c57b0b7f8418198b7615a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/00d956dafa76f86a73424fe5cce3d604a8be2e4b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">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.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)