riscv: fgraph: Fix stack layout to match __arch_ftrace_regs argument of ftrace_return_to_handler

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

Summary

CVE	CVE-2025-22069
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-16 15:16:01 UTC
Updated	2026-04-06 13:43:51 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: riscv: fgraph: Fix stack layout to match __arch_ftrace_regs

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: 0.000920000 probability, percentile 0.257890000 (date 2026-04-07)

Problem Types: CWE-668

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 a3ed4157b7d89800a0008de0c9e46a438a5c3745 78b39c587b8f6c69140177108f9c08a75b1c7c37 gi
CNA	Linux	Linux	affected a3ed4157b7d89800a0008de0c9e46a438a5c3745 67a5ba8f742f247bc83e46dd2313c142b1383276 g
CNA	Linux	Linux	affected 33d4e904e24d14ff0fbc528b657ddc7c7b636e6a git
CNA	Linux	Linux	affected 6.14
CNA	Linux	Linux	unaffected 6.14 semver
CNA	Linux	Linux	unaffected 6.14.2 6.14.* semver
CNA	Linux	Linux	unaffected 6.15 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/67a5ba8f742f247bc83e46dd2313c142b1383276	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/78b39c587b8f6c69140177108f9c08a75b1c7c37	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.