KVM: x86: Add SRCU protection for reading PDPTRs in __get_sregs2()

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

Summary

CVE	CVE-2026-43214
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:40 UTC
Updated	2026-05-11 19:44:24 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Add SRCU protection for reading PDPTRs in _

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 0.024500000 (date 2026-05-12)

Problem Types: NVD-CWE-noinfo

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

ntegrity

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 6dba940352038b56db9b591b172fb2ec76a5fd5e f621ca24f9f489e226e22560761b04884984133b git
CNA	Linux	Linux	affected 6dba940352038b56db9b591b172fb2ec76a5fd5e 708e20c66b2761d878a2bc3c7534e7f814e4dec5 gi
CNA	Linux	Linux	affected 6dba940352038b56db9b591b172fb2ec76a5fd5e 9f2bfea51151dfbb24b52f452eb3d5f5fe0e506e git
CNA	Linux	Linux	affected 6dba940352038b56db9b591b172fb2ec76a5fd5e 57536ff0a6bd69a5808d682925202babdb5ddc13 git
CNA	Linux	Linux	affected 6dba940352038b56db9b591b172fb2ec76a5fd5e b33f8d816950b10e7879cd8ffd7ae4b649ada4db git
CNA	Linux	Linux	affected 6dba940352038b56db9b591b172fb2ec76a5fd5e 95d848dc7e639988dbb385a8cba9b484607cf98c gi
CNA	Linux	Linux	affected 5.14
CNA	Linux	Linux	unaffected 5.14 semver
CNA	Linux	Linux	unaffected 6.1.165 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.128 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.75 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.16 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.6 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/9f2bfea51151dfbb24b52f452eb3d5f5fe0e506e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b33f8d816950b10e7879cd8ffd7ae4b649ada4db	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/57536ff0a6bd69a5808d682925202babdb5ddc13	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/95d848dc7e639988dbb385a8cba9b484607cf98c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f621ca24f9f489e226e22560761b04884984133b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/708e20c66b2761d878a2bc3c7534e7f814e4dec5	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.