x86: shadow stacks: proper error handling for mmap lock

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

Summary

CVE	CVE-2026-43109
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 10:16:24 UTC
Updated	2026-05-11 17:25:58 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: x86: shadow stacks: proper error handling for mmap lock

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

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 7fad2a432cd35bbf104d2d9d426e74902f22aa95 c64cebcc5c4f223dbcbe7dcdf74908fc092a0aa4 git
CNA	Linux	Linux	affected 7fad2a432cd35bbf104d2d9d426e74902f22aa95 262b6d38a81d51b135db81e1f30c13d30e38feee git
CNA	Linux	Linux	affected 7fad2a432cd35bbf104d2d9d426e74902f22aa95 52f657e34d7b21b47434d9d8b26fa7f6778b63a0 git
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 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 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/52f657e34d7b21b47434d9d8b26fa7f6778b63a0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/262b6d38a81d51b135db81e1f30c13d30e38feee	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c64cebcc5c4f223dbcbe7dcdf74908fc092a0aa4	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.