x86/kexec: add a sanity check on previous kernel's ima kexec buffer

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

Summary

CVE	CVE-2026-43240
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 12:16:44 UTC
Updated	2026-05-11 14:27:36 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: x86/kexec: add a sanity check on previous kernel's ima ke

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 b69a2afd5afce9bf6d56e349d6ab592c916e20f2 37f18915a261afe84dab462624ed829cddb77a9b git
CNA	Linux	Linux	affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 22e460b6333a5f818b042ac89201f8e735556f4a git
CNA	Linux	Linux	affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 f8f73bf0f8a57ee9b86792456bd42079bc98c6b7 git
CNA	Linux	Linux	affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 d4a132f121c591b60dbaf57ea91f1faf11631fbc git
CNA	Linux	Linux	affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 4d7a8f5f28187e3d2958b2a134473da2665207e7 git
CNA	Linux	Linux	affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 c5489d04337b47e93c0623e8145fcba3f5739efd git
CNA	Linux	Linux	affected 6.0
CNA	Linux	Linux	unaffected 6.0 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/4d7a8f5f28187e3d2958b2a134473da2665207e7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/d4a132f121c591b60dbaf57ea91f1faf11631fbc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/22e460b6333a5f818b042ac89201f8e735556f4a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c5489d04337b47e93c0623e8145fcba3f5739efd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f8f73bf0f8a57ee9b86792456bd42079bc98c6b7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/37f18915a261afe84dab462624ed829cddb77a9b	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.