



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

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-43240                               |
| <b>State</b>           | PUBLISHED                                    |
| <b>Assigner</b>        | Linux  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback |
| <b>Published</b>       | 2026-05-06 12:16:44 UTC                      |
| <b>Updated</b>         | 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 | <a href="#">Linux</a> | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |

## Vendor Declared Affected Products

| Source | Vendor                | Product               | Version  |
|--------|-----------------------|-----------------------|--|
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 37f18915a261afe84dab462624ed829cddb77a9b git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 22e460b6333a5f818b042ac89201f8e735556f4a git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 f8f73bf0f8a57ee9b86792456bd42079bc98c6b7 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 d4a132f121c591b60dbaf57ea91f1faf11631fbc git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 4d7a8f5f28187e3d2958b2a134473da2665207e7 git |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected b69a2afd5afce9bf6d56e349d6ab592c916e20f2 c5489d04337b47e93c0623e8145fcb3f5739efd git  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | affected 6.0   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.0 semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.1.165 6.1.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.6.128 6.6.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.12.75 6.12.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.18.16 6.18.* semver   |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 6.19.6 6.19.* semver  |
| CNA    | <a href="#">Linux</a> | <a href="#">Linux</a> | unaffected 7.0 * original_commit_for_fix   |

## References

| Reference   | Source                               | Link  | Tags      |
|---|--------------------------------------|---|-----------|
| <a href="https://git.kernel.org/stable/c/4d7a8f5f28187e3d2958b2a134473da2665207e7">git.kernel.org/stable/c/4d7a8f5f28187e3d2958b2a134473da2665207e7</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> | Patch     |
| <a href="https://git.kernel.org/stable/c/d4a132f121c591b60dbaf57ea91f1faf11631fbc">git.kernel.org/stable/c/d4a132f121c591b60dbaf57ea91f1faf11631fbc</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> | Patch     |
| <a href="https://git.kernel.org/stable/c/22e460b6333a5f818b042ac89201f8e735556f4a">git.kernel.org/stable/c/22e460b6333a5f818b042ac89201f8e735556f4a</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> | Patch     |
| <a href="https://git.kernel.org/stable/c/c5489d04337b47e93c0623e8145fcb3f5739efd">git.kernel.org/stable/c/c5489d04337b47e93c0623e8145fcb3f5739efd</a>   | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> | Patch     |
| <a href="https://git.kernel.org/stable/c/f8f73bf0f8a57ee9b86792456bd42079bc98c6b7">git.kernel.org/stable/c/f8f73bf0f8a57ee9b86792456bd42079bc98c6b7</a> | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org">git.kernel.org</a> | Patch     |
| <a href="https://git.kernel.org/stable/c/37f18915a261afe84dab462624ed829cddb77a9b">git.kernel.org/stable/c/37f18915a261afe84dab462624ed829cddb77a9b</a> | 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>       | canonical |
| NVD vulnerability detail  | NVD                                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>     | canonical |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)