



# x86/vmscape: Add conditional IBPB mitigation

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

## Summary

<b>CVE</b>	CVE-2025-40300
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-09-11 17:15:45 UTC
<b>Updated</b>	2026-05-12 13:17:18 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: x86/vmscape: Add conditional IBPB mitigation VMSCAPE

## 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 15d45071523d89b3fb7372e2135fbd72f6af9506 ac60717f9a8d21c58617d0b34274babf24
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 c08192b5d6730a914dee6175bc71092ee6
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 d5490dfa35427a2967e00a4c7a1b95fdbcf
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 2f4f2f8f860cb4c3336a7435ebe8dcfded0c
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 15006289e5c38b2a830e1fba221977a275
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 893387c18612bb452336a5881da0d015a
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 f866eef8d1c65504d30923c3f14082ad294
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 34e5667041050711a947e260fc9ebebe08
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 d7ddc93392e4a7fcccc86edf6ef3e64c778
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 459274c77b37ac63b78c928b4b4e748d1f
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 510603f504796c3535f67f55fb0b124a303l
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 9c23a90648e831d611152ac08dbcd1283c
CNA	Linux	Linux	affected 15d45071523d89b3fb7372e2135fbd72f6af9506 2f8f173413f1cbf52660d04df92d0069c430
CNA	Linux	Linux	affected c51f1e5f57cca88d8d5894b6fad1638f643a99d0 git
CNA	Linux	Linux	affected 4b3870c343a82cd2df7192cc5149c87205dcc611 git
CNA	Linux	Linux	affected 4.16
CNA	Linux	Linux	unaffected 4.16 semver
CNA	Linux	Linux	unaffected 5.10.244 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.193 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.152 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.106 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.47 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.7 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

## References

Reference	Source	Link
git.kernel.org/stable/c/2f8f173413f1cbf52660d04df92d0069c4306d25	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>

<a href="http://www.openwall.com/lists/oss-security/2025/11/14/4">www.openwall.com/lists/oss-security/2025/11/14/4</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="https://git.kernel.org/stable/c/459274c77b37ac63b78c928b4b4e748d1f9d05c8">git.kernel.org/stable/c/459274c77b37ac63b78c928b4b4e748d1f9d05c8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/9c23a90648e831d611152ac08dbcd1283d405e7f">git.kernel.org/stable/c/9c23a90648e831d611152ac08dbcd1283d405e7f</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/f866eef8d1c65504d30923c3f14082ad294d0e6d">git.kernel.org/stable/c/f866eef8d1c65504d30923c3f14082ad294d0e6d</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="http://www.openwall.com/lists/oss-security/2025/11/14/6">www.openwall.com/lists/oss-security/2025/11/14/6</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="https://git.kernel.org/stable/c/510603f504796c3535f67f55fb0b124a303b44c8">git.kernel.org/stable/c/510603f504796c3535f67f55fb0b124a303b44c8</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/ac60717f9a8d21c58617d0b34274babf24135835">git.kernel.org/stable/c/ac60717f9a8d21c58617d0b34274babf24135835</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/d5490dfa35427a2967e00a4c7a1b95fdbc8ede34">git.kernel.org/stable/c/d5490dfa35427a2967e00a4c7a1b95fdbc8ede34</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/15006289e5c38b2a830e1fba221977a27598176c">git.kernel.org/stable/c/15006289e5c38b2a830e1fba221977a27598176c</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="http://www.openwall.com/lists/oss-security/2025/11/14/3">www.openwall.com/lists/oss-security/2025/11/14/3</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="https://git.kernel.org/stable/c/2f4f2f8f860cb4c3336a7435ebe8dcfded0c9c6e">git.kernel.org/stable/c/2f4f2f8f860cb4c3336a7435ebe8dcfded0c9c6e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="http://cert-portal.siemens.com/productcert/html/ssa-032379.html">cert-portal.siemens.com/productcert/html/ssa-032379.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="http://cert-portal.siemens.com">cert-portal.siemens.com</a>
<a href="https://git.kernel.org/stable/c/893387c18612bb452336a5881da0d015a7e8f4a2">git.kernel.org/stable/c/893387c18612bb452336a5881da0d015a7e8f4a2</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/34e5667041050711a947e260fc9e8e8e08bddee5">git.kernel.org/stable/c/34e5667041050711a947e260fc9e8e8e08bddee5</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="http://www.openwall.com/lists/oss-security/2025/11/17/2">www.openwall.com/lists/oss-security/2025/11/17/2</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="https://git.kernel.org/stable/c/d7ddc93392e4a7ffcccc86edf6ef3e64c778db52">git.kernel.org/stable/c/d7ddc93392e4a7ffcccc86edf6ef3e64c778db52</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/c08192b5d6730a914dee6175bc71092ee6a65f14">git.kernel.org/stable/c/c08192b5d6730a914dee6175bc71092ee6a65f14</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="http://www.openwall.com/lists/oss-security/2025/11/17/3">www.openwall.com/lists/oss-security/2025/11/17/3</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.openwall.com">www.openwall.com</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00007.html">lists.debian.org/debian-lts-announce/2025/10/msg00007.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)