



x86/cpu/hygon: Add missing resctrl_cpu_detect() in bsp_init helper

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

Summary

CVE	CVE-2025-39681
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-05 18:15:44 UTC
Updated	2026-05-12 13:17:04 UTC

Description In the Linux kernel, the following vulnerability has been resolved: x86/cpu/hygon: Add missing resctrl_cpu_detect() in bsp_init helper

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 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 62f12cde10118253348a7540e85606869
CNA	Linux	Linux	affected 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 873f32201df8876bdb2563e3187e791494
CNA	Linux	Linux	affected 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 fb81222c1559f89bfe3aa1010f6d112531c
CNA	Linux	Linux	affected 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 7207923d8453ebfb35667c1736169f2dd7
CNA	Linux	Linux	affected 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 a9e5924daa954c9f585c1ca00358afe71c
CNA	Linux	Linux	affected 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 d23264c257a70dbe021b43b3bc2ee1613
CNA	Linux	Linux	affected 923f3a2b48bdccb6a1d1f0dd48de03de7ad936d9 d8df126349dad855cdfedd6bbf315bad2e
CNA	Linux	Linux	affected 5.8
CNA	Linux	Linux	unaffected 5.8 semver
CNA	Linux	Linux	unaffected 5.10.242 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.190 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.44 6.12.* semver
CNA	Linux	Linux	unaffected 6.16.4 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/a9e5924daa954c9f585c1ca00358afe71d6781c4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d8df126349dad855cdfedd6bbf315bad2e901c2f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/62f12cde10118253348a7540e85606869bd69432	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/fb81222c1559f89bfe3aa1010f6d112531d55353	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/d23264c257a70dbe021b43b3bc2ee1613cd2c69	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/7207923d8453ebfb35667c1736169f2dd796772e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/873f32201df8876bdb2563e3187e79149427cab4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org

lists.debian.org/debian-lts-announce/2025/10/msg00007.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report