



# perf/x86/intel: Fix crash in icl\_update\_topdown\_event()

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

## Summary

<b>CVE</b>	CVE-2025-38322
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-07-10 09:15:26 UTC
<b>Updated</b>	2026-05-12 13:16:47 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Fix crash in icl_update_topdown_event() Th

## 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 781b2db0eb7731fbde510c268b7ccc62959c3feb 702ea6028032d6c1fe96c2d4762a3575e9c
CNA	Linux	Linux	affected e7f6922c8a5b41522a8329ea6bbf815993b2dd28 79e2dd573116d3338507c311460da9669
CNA	Linux	Linux	affected 3a8bec6583e5239de3bd597ab382dc6c2b0c29a1 e97c45c770f5e56c784a46c2a96ab968c
CNA	Linux	Linux	affected f9bdf1f953392c9edd69a7f884f78c0390127029 a85cc69acdc05f8cd226b8ea0778b8e2e8
CNA	Linux	Linux	affected f9bdf1f953392c9edd69a7f884f78c0390127029 b0823d5fbacb1c551d793cbfe7af24e0d1fa
CNA	Linux	Linux	affected 06cd7bfb86e9db3e9013ea6636ad2c6f0a1664d git
CNA	Linux	Linux	affected d8370aa704bd7e384918c8f466856374725c0585 git
CNA	Linux	Linux	affected 6.15
CNA	Linux	Linux	unaffected 6.15 semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.101 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.49 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.4 6.15.* semver
CNA	Linux	Linux	unaffected 6.16 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

## References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00008.html">lists.debian.org</a>
git.kernel.org/stable/c/79e2dd573116d3338507c311460da9669095c94d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/79e2dd573116d3338507c311460da9669095c94d">git.kernel.org</a>
git.kernel.org/stable/c/a85cc69acdc05f8cd226b8ea0778b8e2e887e6f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/a85cc69acdc05f8cd226b8ea0778b8e2e887e6f">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-032379.html">cert-portal.siemens.cc</a>
git.kernel.org/stable/c/e97c45c770f5e56c784a46c2a96ab968d26b97d9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/e97c45c770f5e56c784a46c2a96ab968d26b97d9">git.kernel.org</a>
git.kernel.org/stable/c/b0823d5fbacb1c551d793cbfe7af24e0d1fa45ed	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/b0823d5fbacb1c551d793cbfe7af24e0d1fa45ed">git.kernel.org</a>
git.kernel.org/stable/c/702ea6028032d6c1fe96c2d4762a3575e3654819	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/702ea6028032d6c1fe96c2d4762a3575e3654819">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://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](#) 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](#)