# s390/syscalls: Add spectre boundary for syscall dispatch table

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-31483 |
| **State** | PUBLISHED |
| **Assigner** | Linux |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-22 14:16:45 UTC |
| **Updated** | 2026-04-23 16:17:41 UTC |
| **Description** | In the Linux kernel, the following vulnerability has been resolved: s390/syscalls: Add spectre boundary for syscall dispatch t |

## Risk And Classification

**EPSS:** 0.000300000 probability, percentile 0.086370000 (date 2026-04-24)

## Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|---|---|---|---|
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d 3c3b97064764899c39a0abbd35a6caa031e70333 g |
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d 1cb9c7bc9025c637564fabc7fcc3c9343949e310 git |
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d 7a5260fbc6e79a1595328ec5c6aa3f937504a1f0 git |
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d f8c444b918d639e1f9a621ee20fe481c1d10dfc4 git |
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d 87776f02449e3bded95b2ccbd6b012e9ae64e6f3 gi |
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d 4d05dd18d867d58c6952a3bc260d244899da7256 g |
| CNA | Linux | Linux | affected 56e62a73702836017564eaacd5212e4d0fa1c01d 48b8814e25d073dd84daf990a879a820bad2bcbd g |
| CNA | Linux | Linux | affected 5.12 |
| CNA | Linux | Linux | unaffected 5.12 semver |
| CNA | Linux | Linux | unaffected 5.15.203 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.168 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.131 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.12.80 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.18.21 6.18.* semver |
| CNA | Linux | Linux | unaffected 6.19.11 6.19.* semver |
| CNA | Linux | Linux | unaffected 7.0 * original commit for fix |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| git.kernel.org/stable/c/48b8814e25d073dd84daf990a879a820bad2bcbd | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/1cb9c7bc9025c637564fabc7fcc3c9343949e310 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/3c3b97064764899c39a0abbd35a6caa031e70333 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/87776f02449e3bded95b2ccbd6b012e9ae64e6f3 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/7a5260fbc6e79a1595328ec5c6aa3f937504a1f0 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/f8c444b918d639e1f9a621ee20fe481c1d10dfc4 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| git.kernel.org/stable/c/4d05dd18d867d58c6952a3bc260d244899da7256 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

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 registred 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**