



net: sched: fix ets qdisc OOB Indexing

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-21692 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-02-10 16:15:38 UTC |
| Updated | 2026-05-12 13:16:31 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: net: sched: fix ets qdisc OOB Indexing Haowei Yan <g104

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-129 | CWE-129 CWE-129 Improper Validation of Array Index

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1 | nvd@nist.gov | Primary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | ADP | DECLARED | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected dcc68b4d8084e1ac9af0d4022d6b1aff6a139 |
| CNA | Linux | Linux | affected 5.6 |
| CNA | Linux | Linux | unaffected 5.6 semver |
| CNA | Linux | Linux | unaffected 5.10.234 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.178 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.128 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.75 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.12.12 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.13.1 6.13.* semver |
| CNA | Linux | Linux | unaffected 6.14 * original_commit_for_fix |
| ADP | Siemens | RUGGEDCOM RST2428P | affected V3.2 custom |
| ADP | Siemens | SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family | affected V3.2 custom |
| ADP | Siemens | SCALANCE XCM-/XRM-/XCH-/XRH-300 Family | affected V3.2 custom |
| ADP | Siemens | SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem | affected * custom |

References

| Reference | Source | Link |
|--|--------------------------------------|----------------|
| git.kernel.org/stable/c/03c56665dab1f4ac844bc156652d50d639093fa5 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/f4168299e553f17aa2ba4016e77a9c38da40eb1d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |

| | | |
|--|--------------------------------------|------------------------|
| lists.debian.org/debian-lts-announce/2025/03/msg00002.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/1332c6ed446be787f901ed1064ec6a3c694f028a | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| cert-portal.siemens.com/productcert/html/ssa-265688.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.co |
| git.kernel.org/stable/c/997f6ec4208b23c87daf9f044689685f091826f7 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/d62b04fca4340a0d468d7853bd66e511935a18cb | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| lists.debian.org/debian-lts-announce/2025/03/msg00001.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| cert-portal.siemens.com/productcert/html/ssa-355557.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.co |
| git.kernel.org/stable/c/f6b0f05fbfa4044f890e8a348288c0d9a20bd1d0 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/bcf0d815e728a3a304b50455b32a3170c16e1eaa | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.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 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