



Bluetooth: RFCOMM: FIX possible deadlock in rfcomm_sk_state_change

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2024-50044 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-10-21 20:15:17 UTC |
| Updated | 2026-05-12 13:16:16 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: FIX possible deadlock in rfcomm_sk

Risk And Classification

Primary CVSS: v3.1 3.3 LOW from nvd@nist.gov

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

Problem Types: CWE-667

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

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 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 3241ad820dbb172021e0268b56110319914; |
| CNA | Linux | Linux | affected 2.6.27 |
| CNA | Linux | Linux | unaffected 2.6.27 semver |
| CNA | Linux | Linux | unaffected 4.19.323 4.19.* semver |
| CNA | Linux | Linux | unaffected 5.4.285 5.4.* semver |
| CNA | Linux | Linux | unaffected 5.10.227 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.168 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.113 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.57 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.11.4 6.11.* semver |
| CNA | Linux | Linux | unaffected 6.12 * original_commit_for_fix |
| ADP | Siemens | RUGGEDCOM RST2428P | unaffected * custom |
| ADP | Siemens | SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family | unaffected * custom |
| ADP | Siemens | SCALANCE XCM-/XRM-/XCH-/XRH-300 Family | unaffected * custom |
| ADP | Siemens | SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem | affected * custom |

References

| Reference | Source | Link |
|--|--------------------------------------|---|
| git.kernel.org/stable/c/4cb9807c9b53bf1e5560420d26f319f528b50268 | 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/38b2d5a57d125e1c17661b8308c0240c4a43b534 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/ced98072d3511b232ae1d3347945f35f30c0e303 | 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.cc |
| git.kernel.org/stable/c/869c6ee62ab8f01bf2419e45326642be5c9b670a | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/08d1914293dae38350b8088980e59fbc699a72fe | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/ef44274dae9b0a90d1a97ce8b242a3b8243a7745 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| cert-portal.siemens.com/productcert/html/ssa-355557.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.cc |
| lists.debian.org/debian-lts-announce/2025/01/msg00001.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/b77b3fb12fd483cae7c28648903b1d8a6b275f01 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/496b2ab0fd10f205e08909a125485fdc98843dbe | 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