



# pinctl: fix deadlock in create\_pinctl() when handling - EPROBE\_DEFER

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

## Summary

<b>CVE</b>	CVE-2024-42090
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-07-29 17:15:11 UTC
<b>Updated</b>	2026-05-12 12:17:03 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: pinctl: fix deadlock in create\_pinctl() when handling -EPF

## 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:** 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

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 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c7e65a0dc
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c7420ce12
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c7b813e3f
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c701fe2f88
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c7b36efd2
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c74038c57
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c748a7a7c
CNA	Linux	Linux	affected 42fed7ba44e4e8c1fb27b28ad14490cb1daff3c7adec57f
CNA	Linux	Linux	affected 3.10
CNA	Linux	Linux	unaffected 3.10 semver
CNA	Linux	Linux	unaffected 4.19.317 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.279 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.221 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.162 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.97 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.37 6.6.* semver
CNA	Linux	Linux	unaffected 6.9.8 6.9.* semver
CNA	Linux	Linux	unaffected 6.10 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

## References

Reference	Source	Link
git.kernel.org/stable/c/48a7a7c9571c3e62f17012dd7f2063e926179ddd	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/420ce1261907e5dbeda1e4daffd5b6c76f8188c0	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/e65a0dc2e85efb28e182aca50218e8a056d0ce04	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/b36efd2e3e22a329444b6b24fa48df6d20ae66e6	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.co</a>
git.kernel.org/stable/c/adec57ff8e66aee632f3dd1f93787c13d112b7a1	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/01fe2f885f7813f8aed5d3704b384a97b1116a9e	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>

<a href="https://git.kernel.org/stable/c/b813e3fd102a959c5b208ed68afe27e0137a561b">git.kernel.org/stable/c/b813e3fd102a959c5b208ed68afe27e0137a561b</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2025/01/msg00001.html">lists.debian.org/debian-lts-announce/2025/01/msg00001.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/4038c57bf61631219b31f1bd6e92106ec7f084dc">git.kernel.org/stable/c/4038c57bf61631219b31f1bd6e92106ec7f084dc</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">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](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](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)