



# PM / devfreq: Fix buffer overflow in trans\_stat\_show

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

## Summary

<b>CVE</b>	CVE-2023-52614
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-18 11:15:08 UTC
<b>Updated</b>	2026-05-12 12:16:16 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: PM / devfreq: Fix buffer overflow in trans\_stat\_show Fix b

## 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-120

## 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 e552bbaf5b987f57c43e6981a452b8a3c700b1ae 087de0
CNA	Linux	Linux	affected e552bbaf5b987f57c43e6981a452b8a3c700b1ae 796d3f
CNA	Linux	Linux	affected e552bbaf5b987f57c43e6981a452b8a3c700b1ae 8a7729
CNA	Linux	Linux	affected e552bbaf5b987f57c43e6981a452b8a3c700b1ae a979f5
CNA	Linux	Linux	affected e552bbaf5b987f57c43e6981a452b8a3c700b1ae eaef46
CNA	Linux	Linux	affected e552bbaf5b987f57c43e6981a452b8a3c700b1ae 08e23c
CNA	Linux	Linux	affected 3.8
CNA	Linux	Linux	unaffected 3.8 semver
CNA	Linux	Linux	unaffected 5.10.216 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.149 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.76 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.15 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.3 6.7.* semver
CNA	Linux	Linux	unaffected 6.8 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

## References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2024/06/msg00017.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00017.html">lists.debian.org</a>
git.kernel.org/stable/c/087de000e4f8c878c81d9dd3725f00a1d292980c	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/087de000e4f8c878c81d9dd3725f00a1d292980c">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/productcert/html/ssa-265688.html">cert-portal.siemens.com</a>
git.kernel.org/stable/c/08e23d05fa6dc4fc13da0ccf09defdd4bbc92ff4	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/08e23d05fa6dc4fc13da0ccf09defdd4bbc92ff4">git.kernel.org</a>
git.kernel.org/stable/c/a979f56aa4b93579cf0e4265ae04d7e9300fd3e8	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/a979f56aa4b93579cf0e4265ae04d7e9300fd3e8">git.kernel.org</a>
git.kernel.org/stable/c/796d3fad8c35ee9df9027899fb90ceaeb41b958f	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/796d3fad8c35ee9df9027899fb90ceaeb41b958f">git.kernel.org</a>
git.kernel.org/stable/c/8a7729cda2dd276d7a3994638038fb89035b6f2c	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/8a7729cda2dd276d7a3994638038fb89035b6f2c">git.kernel.org</a>
git.kernel.org/stable/c/eaef4650fa2050147ca25fd7ee43bc0082e03c87	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/eaef4650fa2050147ca25fd7ee43bc0082e03c87">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](#)