



# dm: call the resume method on internal suspend

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-26880
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-17 11:15:09 UTC
<b>Updated</b>	2026-05-12 12:16:23 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: dm: call the resume method on internal suspend There is

## 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-476 | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

## 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 fcc39364160663cda1a3c358f4537302a92459b 69836d
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b da7ece
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b f89bd27
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b 03ad5a
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b ad1028
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b 15a3fc5
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b ef02d8e
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b 360a7d
CNA	Linux	Linux	affected fcc39364160663cda1a3c358f4537302a92459b 65e8fbc
CNA	Linux	Linux	affected 3.19
CNA	Linux	Linux	unaffected 3.19 semver
CNA	Linux	Linux	unaffected 4.19.311 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.273 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.214 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.153 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.83 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.23 6.6.* semver
CNA	Linux	Linux	unaffected 6.7.11 6.7.* semver
CNA	Linux	Linux	unaffected 6.8.2 6.8.* semver
CNA	Linux	Linux	unaffected 6.9 * original_commit_for_fix
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.0 V3.1.5 custom

## References

Reference	Source	Link
<a href="https://cert-portal.siemens.com/productcert/html/ssa-398330.html">cert-portal.siemens.com/productcert/html/ssa-398330.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-398330.html">cert-portal.siemens.com</a>
<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00017.html">lists.debian.org/debian-lts-announce/2024/06/msg00017.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00017.html">lists.debian.org</a>
<a href="https://git.kernel.org/stable/c/65e8fbde64520001abf1c8d0e573561b4746ef38">git.kernel.org/stable/c/65e8fbde64520001abf1c8d0e573561b4746ef38</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/65e8fbde64520001abf1c8d0e573561b4746ef38">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/15a3fc5c8774c17589dabfe1d642d40685c985af">git.kernel.org/stable/c/15a3fc5c8774c17589dabfe1d642d40685c985af</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/15a3fc5c8774c17589dabfe1d642d40685c985af">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/f89bd27709376d37ff883067193320c58a8c1d5a">git.kernel.org/stable/c/f89bd27709376d37ff883067193320c58a8c1d5a</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/f89bd27709376d37ff883067193320c58a8c1d5a">git.kernel.org</a>
<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.com/productcert/html/ssa-265688.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com/productcert/html/ssa-265688.html">cert-portal.siemens.com</a>
<a href="https://git.kernel.org/stable/c/69836d9329f0b4c58faaf3d886a7748ddb5bf718">git.kernel.org/stable/c/69836d9329f0b4c58faaf3d886a7748ddb5bf718</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/69836d9329f0b4c58faaf3d886a7748ddb5bf718">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/ef02d8edf738557af2865c5bfb66a03c4e071be7">git.kernel.org/stable/c/ef02d8edf738557af2865c5bfb66a03c4e071be7</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/ef02d8edf738557af2865c5bfb66a03c4e071be7">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/03ad5ad53e51abf3a4c7538c1bc67a5982b41dc5">git.kernel.org/stable/c/03ad5ad53e51abf3a4c7538c1bc67a5982b41dc5</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/03ad5ad53e51abf3a4c7538c1bc67a5982b41dc5">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/ad10289f68f45649816cc68eb93f45fd5ec48a15">git.kernel.org/stable/c/ad10289f68f45649816cc68eb93f45fd5ec48a15</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/ad10289f68f45649816cc68eb93f45fd5ec48a15">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/da7ece2197101b1469853e6b5e915be1e3896d52">git.kernel.org/stable/c/da7ece2197101b1469853e6b5e915be1e3896d52</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/da7ece2197101b1469853e6b5e915be1e3896d52">git.kernel.org</a>
<a href="https://git.kernel.org/stable/c/360a7d1be8112654f1fb328ed3862be630bca3f4">git.kernel.org/stable/c/360a7d1be8112654f1fb328ed3862be630bca3f4</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org/stable/c/360a7d1be8112654f1fb328ed3862be630bca3f4">git.kernel.org</a>
<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00020.html">lists.debian.org/debian-lts-announce/2024/06/msg00020.html</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org/debian-lts-announce/2024/06/msg00020.html">lists.debian.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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

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)