



# apparmor: fix unprivileged local user can do privileged policy management

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

## Summary

<b>CVE</b>	CVE-2026-23268
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-18 18:16:25 UTC
<b>Updated</b>	2026-04-02 15:16:27 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: apparmor: fix unprivileged local user can do privileged pol

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected b7fd2c0340eacbee892425e9007647568b7f2a3c 17debf5586020790b5717f96e5e6a3ca5bb961ab git
CNA	Linux	Linux	affected b7fd2c0340eacbee892425e9007647568b7f2a3c 0fc63dd9170643d15c25681fca792539e23f4640 git
CNA	Linux	Linux	affected b7fd2c0340eacbee892425e9007647568b7f2a3c b60b3f7a35c46b2e0ca934f9c988b8fca06d76c6 git
CNA	Linux	Linux	affected b7fd2c0340eacbee892425e9007647568b7f2a3c b6a94eeca9c6c8f7c55ad44c62c98324f51ec596 git
CNA	Linux	Linux	affected b7fd2c0340eacbee892425e9007647568b7f2a3c 6601e13e82841879406bf9f369032656f441a425 git
CNA	Linux	Linux	affected 4.11
CNA	Linux	Linux	unaffected 4.11 semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.77 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.18 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.8 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc4 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/6601e13e82841879406bf9f369032656f441a425	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
www.qualys.com/2026/03/10/crack-armor.txt	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://www.qualys.com">www.qualys.com</a>	
git.kernel.org/stable/c/b6a94eeca9c6c8f7c55ad44c62c98324f51ec596	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/b60b3f7a35c46b2e0ca934f9c988b8fca06d76c6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/0fc63dd9170643d15c25681fca792539e23f4640	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/17debf5586020790b5717f96e5e6a3ca5bb961ab	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<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>	cano
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**