



apparmor: validate DFA start states are in bounds in unpack_pdb

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

Summary

CVE	CVE-2026-23269
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-18 18:16:25 UTC
Updated	2026-04-02 15:16:27 UTC

Description In the Linux kernel, the following vulnerability has been resolved: apparmor: validate DFA start states are in bounds in unpa

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000320000 probability, percentile 0.091780000 (date 2026-04-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ad5ff3db53c68c2f12936bc74ea5dfe0af943592 07cf6320f40ea2ccfad63728cff34ecb309d03da git
CNA	Linux	Linux	affected ad5ff3db53c68c2f12936bc74ea5dfe0af943592 15c3eb8916e7db01cb246d04a1fe6f0fdc065b0c git
CNA	Linux	Linux	affected ad5ff3db53c68c2f12936bc74ea5dfe0af943592 0baadb0eece2c4d939db10d3c323b4652ac79a58 git
CNA	Linux	Linux	affected ad5ff3db53c68c2f12936bc74ea5dfe0af943592 3bb7db43e32190c973d4019037cedb7895920184 git
CNA	Linux	Linux	affected ad5ff3db53c68c2f12936bc74ea5dfe0af943592 9063d7e2615f4a7ab321de6b520e23d370e58816 git
CNA	Linux	Linux	affected 3.4
CNA	Linux	Linux	unaffected 3.4 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	Tag
git.kernel.org/stable/c/07cf6320f40ea2ccfad63728cff34ecb309d03da	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
www.qualys.com/2026/03/10/crack-armor.txt	416baaa9-dc9f-4396-8d5f-8c081fb06d67	www.qualys.com	
git.kernel.org/stable/c/0baadb0eece2c4d939db10d3c323b4652ac79a58	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9063d7e2615f4a7ab321de6b520e23d370e58816	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3bb7db43e32190c973d4019037cedb7895920184	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/15c3eb8916e7db01cb246d04a1fe6f0fdc065b0c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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](#).

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