



net: shaper: protect late read accesses to the hierarchy

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

Summary

CVE	CVE-2026-23437
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 16:16:25 UTC
Updated	2026-04-27 14:16:32 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: net: shaper: protect late read accesses to the hierarchy W

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

EPSS: 0.000170000 probability, percentile 0.039750000 (date 2026-04-07)

Problem Types: NVD-CWE-noinfo

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	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

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 4b623f9f0f59652ea71fcb27d60b4c3b65126dbb 581eee0890a8bde44f1fb78ad3e70502a897d583 git
CNA	Linux	Linux	affected 4b623f9f0f59652ea71fcb27d60b4c3b65126dbb 348758ba74e6a348299965b16a97cfb817545cc0 git
CNA	Linux	Linux	affected 4b623f9f0f59652ea71fcb27d60b4c3b65126dbb 0f9ea7141f365b4f27226898e62220fb98ef8dc6 git
CNA	Linux	Linux	affected 6.13
CNA	Linux	Linux	unaffected 6.13 semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References				
Reference	Source	Link	Tags	
git.kernel.org/stable/c/581eee0890a8bde44f1fb78ad3e70502a897d583	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch	
git.kernel.org/stable/c/348758ba74e6a348299965b16a97cfb817545cc0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch	
git.kernel.org/stable/c/0f9ea7141f365b4f27226898e62220fb98ef8dc6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch	
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical	

No vendor comments have been submitted for this CVE.

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

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