



media: dvb-core: fix wrong reinitialization of ringbuffer on reopen

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

Summary

CVE	CVE-2026-23253
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-18 18:16:23 UTC
Updated	2026-04-02 15:16:27 UTC

Description In the Linux kernel, the following vulnerability has been resolved: media: dvb-core: fix wrong reinitialization of ringbuffer on r

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 34731df288a5ffe4b0c396caf8cd24c6a710a222 f1e520ca2e83ece6731af6167c9e5e16931ecba0 git
CNA	Linux	Linux	affected 34731df288a5ffe4b0c396caf8cd24c6a710a222 af050ab44fa1b1897a940d7d756e512232f5e5df git
CNA	Linux	Linux	affected 34731df288a5ffe4b0c396caf8cd24c6a710a222 d71781bad59b1c9d60d7068004581f9bf19c0c9d git
CNA	Linux	Linux	affected 34731df288a5ffe4b0c396caf8cd24c6a710a222 cfd94642025e6f71c8f754bdec0800ee95e4f3dd git
CNA	Linux	Linux	affected 34731df288a5ffe4b0c396caf8cd24c6a710a222 32eb8e4adc207ef31bc6e5ae56bab940b0176066 git
CNA	Linux	Linux	affected 34731df288a5ffe4b0c396caf8cd24c6a710a222 bfbc0b5b32a8f28ce284add619bf226716a59bc0 git
CNA	Linux	Linux	affected 2.6.17
CNA	Linux	Linux	unaffected 2.6.17 semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* 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 6.18.17 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.7 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc2 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/f1e520ca2e83ece6731af6167c9e5e16931ecba0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/af050ab44fa1b1897a940d7d756e512232f5e5df	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d71781bad59b1c9d60d7068004581f9bf19c0c9d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/32eb8e4adc207ef31bc6e5ae56bab940b0176066	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cfd94642025e6f71c8f754bdec0800ee95e4f3dd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/bfbc0b5b32a8f28ce284add619bf226716a59bc0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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](#)