



# drm/amdgpu: Fix error handling in slot reset

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

## Summary

<b>CVE</b>	CVE-2026-23358
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 11:16:34 UTC
<b>Updated</b>	2026-04-24 19:03:35 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix error handling in slot reset If the device f

## 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-908

## 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 732c6cefc1ecfc8de5d7a2029480798655d979d8 73e8bdf14248136459753252a438177df7ed8c7c git
CNA	Linux	Linux	affected 732c6cefc1ecfc8de5d7a2029480798655d979d8 baf4e7968911635eb816870af0ea587ac1457052 git
CNA	Linux	Linux	affected 732c6cefc1ecfc8de5d7a2029480798655d979d8 b57c4ec98c17789136a4db948aec6daadceb5024 gi
CNA	Linux	Linux	affected 6.16
CNA	Linux	Linux	unaffected 6.16 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 * original_commit_for_fix

## References

Reference	Source	Link	Tags
git.kernel.org/stable/c/b57c4ec98c17789136a4db948aec6daadceb5024	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/b57c4ec98c17789136a4db948aec6daadceb5024">git.kernel.org</a>	Patch
git.kernel.org/stable/c/73e8bdf14248136459753252a438177df7ed8c7c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/73e8bdf14248136459753252a438177df7ed8c7c">git.kernel.org</a>	Patch
git.kernel.org/stable/c/baf4e7968911635eb816870af0ea587ac1457052	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org/stable/c/baf4e7968911635eb816870af0ea587ac1457052">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

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)