



# CVE-2024-36333

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-36333
<b>State</b>	PUBLISHED
<b>Assigner</b>	AMD
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-15 05:16:32 UTC
<b>Updated</b>	2026-05-15 05:16:32 UTC
<b>Description</b>	A DLL hijacking vulnerability in the AMD Cleanup Utility could allow an attacker to achieve privilege escalation potentially re

## Risk And Classification

**Primary CVSS:** v4.0 7 HIGH from psirt@amd.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** Security Vulnerability

Version	Source	Type	Score	Severity	Vector
4.0	psirt@amd.com	Secondary	7	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	AMD	<a href="#">AMD Radeon RX 5000 Series Graphics Products</a>	unaffected AMD Software: Adrenalin Edition 25.10.2 (25.20.2)
CNA	AMD	<a href="#">AMD Radeon PRO W5000 Series Graphics Products</a>	unaffected AMD Software: PRO Edition 25.Q3.1 (25.10.32 R)
CNA	AMD	<a href="#">AMD Radeon RX 6000 Series Graphics Products</a>	unaffected AMD Software: Adrenalin Edition 25.10.2 (25.20.2)
CNA	AMD	<a href="#">AMD Radeon RX 7000 Series Graphics Products</a>	unaffected AMD Software: Adrenalin Edition 25.10.2 (25.20.2)
CNA	AMD	<a href="#">AMD Cleanup Utility</a>	unaffected <a href="https://www.amd.com/en/resources/support-article">https://www.amd.com/en/resources/support-article</a>
CNA	AMD	<a href="#">AMD Radeon PRO W6000 Series Graphics Products</a>	unaffected AMD Software: PRO Edition 25.Q3.1 (25.10.32 R)
CNA	AMD	<a href="#">AMD Radeon PRO W7000 Series Graphics Products</a>	unaffected AMD Software: PRO Edition 25.Q3.1 (25.10.32 R)
CNA	AMD	<a href="#">AMD Radeon RX Vega Series Graphics Cards</a>	unaffected AMD Software: Adrenalin Edition 26.1.1 (23.19.24)
CNA	AMD	<a href="#">AMD Radeon VII</a>	unaffected AMD Software: Adrenalin Edition 26.1.1 (23.19.24)
CNA	AMD	<a href="#">AMD Radeon PRO WX 8000/9000 Series Graphics Cards</a>	unaffected AMD Software: PRO Edition 26.Q1 (23.19.24)
CNA	AMD	<a href="#">AMD Radeon PRO VII</a>	unaffected AMD Software: PRO Edition 26.Q1 (23.19.24)

### References

Reference	Source	Link	Tags
<a href="http://www.amd.com/en/resources/product-security/bulletin/AMD-SB-6027.html">www.amd.com/en/resources/product-security/bulletin/AMD-SB-6027.html</a>	psirt@amd.com	<a href="http://www.amd.com">www.amd.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Reported through AMD Bug Bounty Program (en)

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](#).

**Free CVE JSON API** [cve.report/api](#)

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