



# CVE-2022-23831

Published on: Not Yet Published

Last Modified on: 03/01/2023 06:04:00 PM UTC

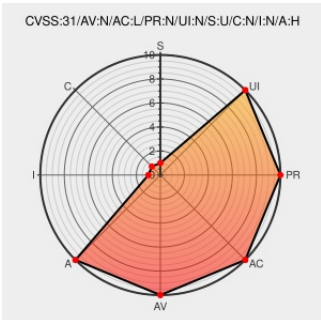
## CVE-2022-23831 - advisory for AMD-SB-1046

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Amd Uprof](#) from [Amd](#) contain the following vulnerability:

Insufficient validation of the IOCTL input buffer in AMD  $\mu$ Prof may allow an attacker to send an arbitrary buffer leading to a potential Windows kernel crash resulting in denial of service.

CVE-2022-23831 has been assigned by [psirt@amd.com](mailto:psirt@amd.com) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [AMD](#) - AMD  $\mu$ Prof version < 3.6.549

Affected Vendor/Software: [AMD](#) - AMD  $\mu$ Prof version < 3.6.839

Affected Vendor/Software: [AMD](#) - AMD  $\mu$ Prof version < 3.6-449

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>NONE</b>	<b>NONE</b>	<b>HIGH</b>

## CVE References

Description	Tags	Link
<b>No Description Provided</b>	<a href="http://www.amd.com">www.amd.com</a>	<a href="https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046">MISC www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046</a>
	<b>Inactive Link</b> <b>Not Archived</b>	

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

#### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Amd</a>	<a href="#">Amd Uprof</a>	All	All	All	All
Operating System	<a href="#">Freebsd</a>	<a href="#">Freebsd</a>	-	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All

cpe:2.3:a:amd:amd\_uprof:\*.\*\*\*.\*\*\*.\*\*\*:


cpe:2.3:o:freebsd:freebsd:-\*.\*\*\*.\*\*\*.\*\*\*:

cpe:2.3:o:linux:linux\_kernel:-\*.\*\*\*.\*\*\*.\*\*\*:

cpe:2.3:o:microsoft:windows:-\*.\*\*\*.\*\*\*.\*\*\*:

No vendor comments have been submitted for this CVE

#### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-23831 : Insufficient validation of the IOCTL input buffer in AMD µProf may allow an attacker to send an ar... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-11-09 21:07:55

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](https://status.cve.report)