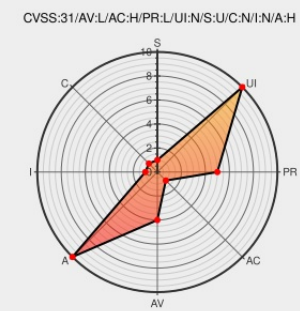
CVE-2021-46795

Published on: Not Yet Published

Last Modified on: 01/20/2023 06:36:00 PM UTC

CVE-2021-46795 - advisory for AMD-SB-1031

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cezannepi-fp6 from Amd contain the following vulnerability:

A TOCTOU (time-of-check to time-of-use) vulnerability exists where an attacker may use a compromised BIOS to cause the TEE OS to read memory out of bounds that could potentially result in a denial of service.

CVE-2021-46795 has been assigned by psirt@amd.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **AMD** - **Ryzen 5000 Series** version **= various**

Affected Vendor/Software: **AMD** - **Ryzen 3000 Series** version **= various**

CVSS3 Score: 4.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
No Description Provided	www.amd.com Inactive Link Not Archived	MISC www.amd.com/en/corporate/product-security/bulletin/AMD-SB-1031

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A TOCTOU (time-of-check to time-of-use) vulnerability exists where an attacker may use a compromised BIOS to cause th…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Amd	Cezannepi-fp6	-	All	All	All
Operating System	Amd	Cezannepi-fp6 Firmware	All	All	All	All
Hardware	Amd	Comboam4v2 Pi	-	All	All	All
Operating System	Amd	Comboam4v2 Pi Firmware	All	All	All	All
Operating System	Amd	Renoirpi-fp6 Firmware	All	All	All	All

cpe:2.3:h:amd:cezannepi-fp6:-:*:*:*:*:*:*:*:

cpe:2.3:o:amd:cezannepi-fp6_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:amd:comboam4v2_pi:-:*:*:*:*:*:*:*:

cpe:2.3:o:amd:comboam4v2_pi_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:amd:renoirpi-fp6_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-46795 : A TOCTOU time-of-check to time-of-use vulnerability exists where an attacker may use a compromis… twitter.com/i/web/status/1…	2023-01-11 08:17:05
/r/netcve	CVE-2021-46795	2023-01-11 08:39:03

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report