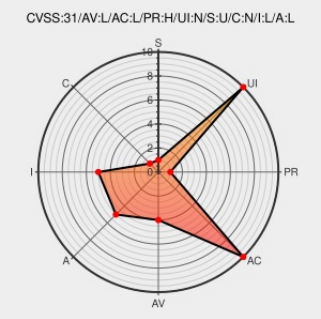
CVE-2022-41597

Published on: Not Yet Published

Last Modified on: 10/15/2022 01:55:00 AM UTC

CVE-2022-41597

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



Certain versions of Emui from Huawei contain the following vulnerability:

The phones have the heap overflow, out-of-bounds read, and null pointer vulnerabilities in the fingerprint trusted application (TA).Successful exploitation of this vulnerability may affect the fingerprint service.

CVE-2022-41597 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **Huawei** - **HarmonyOS** version **= 2.0**

Affected Vendor/Software: **Huawei** - **EMUI** version **= 12.0.0**

Affected Vendor/Software: **Huawei** - **EMUI** version **= 11.0.1**

CVSS3 Score: 3.4 - LOW

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

CVE References

Description	Tags	Link
October	consumer.huawei.com text/html	MISC consumer.huawei.com/en/support/bulletin/2022/10/
文档中心	device.harmonyos.com text/html	MISC device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202210-0000001416095697

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Huawei	Emui	11.0.1	All	All	All
Operating System	Huawei	Emui	12.0.0	All	All	All
Operating System	Huawei	Harmonyos	2.0	All	All	All

cpe:2.3:o:huawei:emui:11.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:emui:12.0.0:*:*:*:*:*:*:*:

cpe:2.3:o:huawei:harmonyos:2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→