



CVE-2022-48301

Published on: Not Yet Published

Last Modified on: 02/17/2023 01:04:00 PM UTC

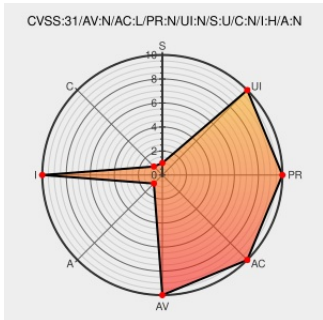
CVE-2022-48301

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Emui** from **Huawei** contain the following vulnerability:

The bundle management module lacks permission verification in some APIs. Successful exploitation of this vulnerability may restore the pre-installed apps that have been uninstalled.

CVE-2022-48301 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Document	device.harmonyos.com text/html	MISC device.harmonyos.com/en/docs/security/update/security-bulletins-202302-0000001454769474
February	consumer.huawei.com text/html	MISC consumer.huawei.com/en/support/bulletin/2023/2/

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.

There are currently no QIDs associated with this CVE

The bundle management module lacks permission verification in some APIs. Successful exploitation of this vulnerabilit...

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	Emui	12.0.1	All	All	All
Operating System	Huawei	Harmonyos	2.0	All	All	All
Operating System	Huawei	Harmonyos	2.1.0	All	All	All
Operating System	Huawei	Harmonyos	3.0.0	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:emui:12.0.1:****:***:						
cpe:2.3:o:huawei:harmonyos:2.0:****:***:						
cpe:2.3:o:huawei:harmonyos:2.1.0:****:***:						
cpe:2.3:o:huawei:harmonyos:3.0.0:****:***:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-48301 : The bundle management module lacks permission verification in some APIs. Successful exploitation o... twitter.com/i/web/status/1...	2023-02-09 17:12:30
 /r/netcve	CVE-2022-48301	2023-02-09 18:38:38

← Previous ID

Next ID→

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](#)