



CVE-2021-40012

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2021-40012

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Vulnerability of pointers being incorrectly used during data transmission in the video framework. Successful exploitation of this vulnerability may affect confidentiality.

CVE-2021-40012 has been assigned by psirt@huawei.com to track the vulnerability - currently rated as **HIGH** severity.

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

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

Affected Vendor/Software: **Huawei** - **EMUI** version = **11.0.0**

Affected Vendor/Software: **Huawei** - **Magic UI** version = **4.0.0**

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	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
August	consumer.huawei.com text/html	 MISC consumer.huawei.com/en/support/bulletin/2022/8/
HUAWEI EMUI/Magic UI security updates July 2022	consumer.huawei.com text/html	 MISC consumer.huawei.com/en/support/bulletin/2022/7/
Document	device.harmonyos.com text/html	 MISC device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202208-0000001363876177

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

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
Operating System	Huawei	Emui	11.0.0	All	All	All
Operating System	Huawei	Emui	12.0.0	All	All	All
Operating System	Huawei	Harmonyos	2.0	All	All	All
Operating System	Huawei	Magic Ui	4.0.0	All	All	All
cpe:2.3:o:huawei:emui:11.0.0:****:****:						
cpe:2.3:o:huawei:emui:12.0.0:****:****:						
cpe:2.3:o:huawei:harmonyos:2.0:****:****:						
cpe:2.3:o:huawei:magic_ui:4.0.0:****:****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-40012 : Vulnerability of pointers being incorrectly used during data transmission in the video framework.... twitter.com/i/web/status/1...	2022-07-12 14:09:02

[← 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](#)