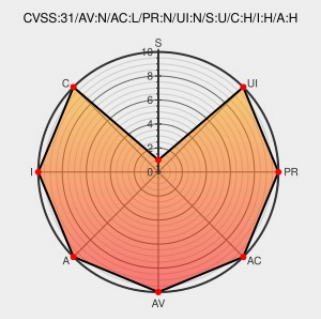
CVE-2020-26707

Published on: 10/31/2021 12:00:00 AM UTC

Last Modified on: 05/03/2022 04:04:00 PM UTC

CVE-2020-26707

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



Certain versions of Aaptjs from Aaptjs Project contain the following vulnerability:

An issue was discovered in the add function in Shenzhim AAPTJS 1.3.1 which allows attackers to execute arbitrary code via the filePath parameter.

CVE-2020-26707 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Remote Code Execution(RCE) via insecure command formatting · Issue #2 · shenzhim/aaptjs · GitHub	github.com text/html	MISC github.com/shenzhim/aaptjs/issues/2

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aaptjs Project	Aaptjs	1.3.1	All	All	All

cpe:2.3:a:aaptjs_project:aaptjs:1.3.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-26707 : An issue was discovered in the add function in Shenzhim AAPTJS 1.3.1 which allows attackers to exe… twitter.com/i/web/status/1…	2021-10-31 20:03:10

← Previous ID

Next ID→