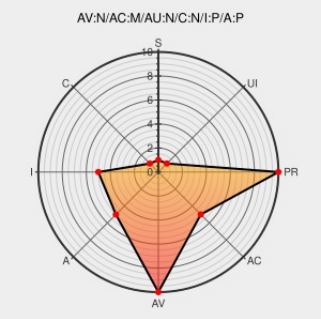
CVE-2014-1969

Published on: 04/11/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-1969

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



Certain versions of Sd Card Manager from Apps4u@android contain the following vulnerability:

Directory traversal vulnerability in the apps4u@android SD Card Manager application before 20140224 for Android allows attackers to overwrite or create arbitrary files via a crafted filename.

CVE-2014-1969 has been assigned by vultures@jpcert.or.jp to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
JVN#47386847: SD Card Manager vulnerable to directory traversal	jvn.jp, text/xml	JVN JVN#47386847
No Description Provided	jvndb.jvn.jp, text/html	JVNDB JVNDB-2014-000035

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apps4u@android	Sd Card Manager	All	All	All	All
Application	Apps4u@android	Sd Card Manager	All	All	All	All

cpe:2.3:a:apps4u@android:sd_card_manager:*:*:*:*:*:android:*:*:

cpe:2.3:a:apps4u\@android:sd_card_manager:*:*:*:*:*:android:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→