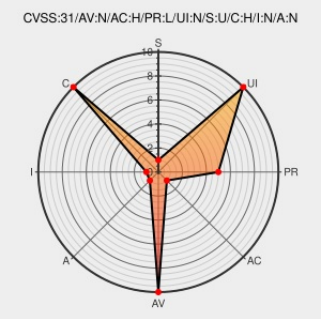
CVE-2021-32754

Published on: 07/12/2021 12:00:00 AM UTC

Last Modified on: 07/15/2021 04:31:00 PM UTC

CVE-2021-32754 - advisory for GHSA-39r7-275f-rvgw

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



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

FlowDroid is a data flow analysis tool. FlowDroid versions prior to 2.9.0 contained an XML external entity (XXE) vulnerability that allowed an attacker who had control over the source/sink definition file in XML format to read files from external locations. In order for this to occur, the XML-based format for sources and sinks had to be used and the attacker had to able control the source/sink definition file. The vulnerability was patched in version 2.9.0. As a workaround, do not allow untrusted entities to control the source/sink definition file.

CVE-2021-32754 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **secure-software-engineering** - **FlowDroid** version **< 2.9.0**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
Improper Restriction of XML External Entity Reference in de.tud.sse · Advisory · secure-software-engineering/FlowDroid · GitHub	github.com text/html	CONFIRM github.com/secure-software-engineering/FlowDroid/security/advisories/GHSA-39r7-275f-rvgw

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	Flowdroid Project	Flowdroid	All	All	All	All

cpe:2.3:a:flowdroid_project:flowdroid:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32754 : FlowDroid is a data flow analysis tool. FlowDroid versions prior to 2.9.0 contained an XML externa… twitter.com/i/web/status/1…	2021-07-12 23:06:13
/r/netcve	CVE-2021-32754	2021-07-12 23:41:03

← Previous ID

Next ID→