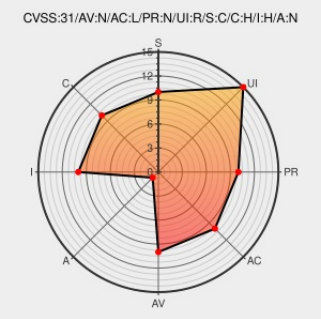
CVE-2021-21386

Published on: 03/24/2021 12:00:00 AM UTC

Last Modified on: 03/27/2021 01:48:00 AM UTC

CVE-2021-21386 - advisory for GHSA-8434-v7xw-8m9x

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



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

APKLeaks is an open-source project for scanning APK file for URIs, endpoints & secrets. APKLeaks prior to v2.0.3 allows remote attackers to execute arbitrary OS commands via package name inside application manifest. An attacker could include arguments that allow unintended commands or code to be executed, allow sensitive data to be read or modified or could cause other unintended behavior through malicious package name. The problem is fixed in version v2.0.6-dev and above.

CVE-2021-21386 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **dwisiswant0** - **apkleaks** version **< 2.0.6-dev**

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: 10 - HIGH

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

CVE References

Description	Tags	Link
Improper Neutralization of Argument Delimiters in a Decompiling Package Process · Advisory · dwisiswant0/apkleaks · GitHub	github.com text/html	CONFIRM github.com/dwisiswant0/apkleaks/security/advisories/GHSA-8434-v7xw-8m9x
Escapes decompiling arguments · dwisiswant0/apkleaks@a966e78 · GitHub	github.com text/html	MISC github.com/dwisiswant0/apkleaks/commit/a966e781499ff6fd4eea66876d7532301b13a382

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apkleaks Project	Apkleaks	All	All	All	All

cpe:2.3:a:apkleaks_project:apkleaks:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→