



CVE-2020-27030

Published on: 12/15/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-27030

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

In onCreate of HandleApiCalls.java, there is a possible permission bypass due to a confused deputy. This could lead to local escalation of privilege that allows an app to set or dismiss the alarm with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-11 Android ID: A-150612638

CVE-2020-27030 has been assigned by security@android.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
Pixel Update Bulletin—December 2020 Android Open Source Project	Vendor Advisory source.android.com	MISC source.android.com/security/bulletin/pixel/2020-12-

