



CVE-2019-2200

Published on: 02/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:04 PM UTC

CVE-2019-2200

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

In updatePermissions of PermissionManagerService.java, it may be possible for a malicious app to obtain a custom permission from another app due to a permission bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation. Product: Android Versions:

Android-10 Android ID: A-67319274

CVE-2019-2200 has been assigned by security@android.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Android Security Bulletin—February 2020 Android Open Source Project	Patch Vendor Advisory	MISC source.android.com/security/bulletin/2020-02-01

text/html

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	10.0	All	All	All
Operating System	Google	Android	10.0	All	All	All
cpe:2.3:o:google:android:10.0:****:*:*:						
cpe:2.3:o:google:android:10.0:****:*:*:						

[← Previous ID](#)

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE.report and Source URL Uptime Status status.cve.report