

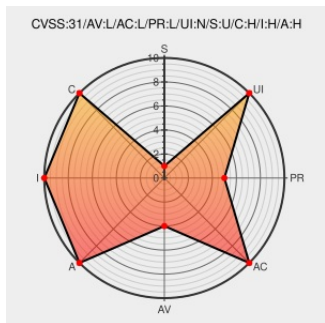


CVE-2020-0081

Published on: 04/17/2020 12:00:00 AM UTC

Last Modified on: 05/03/2022 02:21:00 PM UTC

CVE-2020-0081

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

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

In finalize of AssetManager.java, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0 Android-8.1 Android-9 Android-10 Android ID: A-144028297

CVE-2020-0081 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: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 32 Update: nextcloud-18.0.9-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-c9863904de
Android Security Bulletin—April 2020 Android Open Source Project	Vendor Advisories	MISC

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Google	Android	10.0	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All
Operating System	Google	Android	10.0	All	All	All
Operating System	Google	Android	8.0	All	All	All
Operating System	Google	Android	8.1	All	All	All
Operating System	Google	Android	9.0	All	All	All
cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*.*						
cpe:2.3:o:google:android:10.0:*:*:*:*:*.*						
cpe:2.3:o:google:android:8.0:*:*:*:*:*.*						
cpe:2.3:o:google:android:8.1:*:*:*:*:*.*						
cpe:2.3:o:google:android:9.0:*:*:*:*:*.*						
cpe:2.3:o:google:android:10.0:*:*:*:*:*.*						
cpe:2.3:o:google:android:8.0:*:*:*:*:*.*						
cpe:2.3:o:google:android:8.1:*:*:*:*:*.*						
cpe:2.3:o:google:android:9.0:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)