

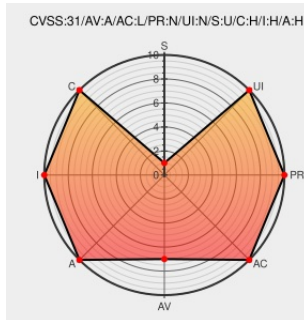


CVE-2020-5764

Published on: 07/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5764

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

Certain versions of **Mx Player** from **Mxplayer** contain the following vulnerability:

MX Player Android App versions prior to v1.24.5, are vulnerable to a directory traversal vulnerability when user is using the MX Transfer feature in "Receive" mode. An attacker can exploit this by connecting to the MX Transfer session as a "sender" and sending a MessageType of "FILE_LIST" with a "name" field containing directory traversal

characters (../). This will result in the file being transferred to the victim's phone, but being saved outside of the intended "/sdcard/MXshare" directory. In some instances, an attacker can achieve remote code execution by writing ".odex" and ".vdex" files in the "oat" directory of the MX Player application.

CVE-2020-5764 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description

MX Player Android App Directory Traversal - Research Advisory | Tenable®

Tags

Exploit

Third Party Advisory

www.tenable.com

text/html

Link

MISC

www.tenable.com/security/research/tra-2020-41

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	Mxplayer	Mx Player	All	All	All	All
Application	Mxplayer	Mx Player	All	All	All	All

cpe:2.3:a:mxplayer:mx_player:*:*:*:*:android:*:*:

cpe:2.3:a:mxplayer:mx_player:*:*:*:*:android:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →