



CVE-2020-12731

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-12731
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-15 15:15:00 UTC
Updated	2021-08-03 16:49:00 UTC
Description	The MagicMotion Flamingo 2 application for Android stores data on an sdcard under com.vt.magicmotion/files/Pictures, wh

Risk And Classification

Problem Types: CWE-312

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Magicmotion	Flamingo 2	-	All	All	All
Operating System	Magicmotion	Flamingo 2 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Magic Flamingo - MagicMotion	MISC	www.magicsmotion.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

630736 For Android Vulnerability CVE-2020-12731

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](#).

Free CVE JSON API cve.report/api

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