



CVE-2018-9515

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

Summary

CVE	CVE-2018-9515
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-02 19:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In sdcardfs_create and sdcardfs_mkdir of inode.c, there is a possible memory corruption due to improper locking. This could lead to a denial of service (DoS) or a remote code execution (RCE) if an attacker can exploit the vulnerability.

Risk And Classification

Problem Types: CWE-119 | NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All

References

Reference	Source	Link	Tags
Android Security Bulletin—October 2018 Android Open Source Project	CONFIRM	source.android.com	Vendor Adv
Google Android Kernel Components Multiple Privilege Escalation Vulnerabilities	BID	www.securityfocus.com	Third Party
Android - sdcardfs Changes current->fs Without Proper Locking - Android dos Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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