



CVE-2017-0520

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

Summary

CVE	CVE-2017-0520
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-08 01:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An elevation of privilege vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to ex

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.10	All	All	All
Operating System	Linux	Linux Kernel	3.18	All	All	All
Operating System	Linux	Linux Kernel	3.10	All	All	All
Operating System	Linux	Linux Kernel	3.18	All	All	All

References

Reference
Google Nexus Qualcomm Crypto Engine Driver CVE-2017-0520 Privilege Escalation Vulnerability
Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users
kernel/msm-3.18 - Unnamed repository
Android Security Bulletin—March 2017 Android Open Source Project
Android Security Bulletin—March 2017 Android Open Source Project
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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