



CVE-2017-13216

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

Summary

CVE	CVE-2017-13216
State	PUBLIC
Assigner	security@android.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-12 23:29:00 UTC
Updated	2018-01-30 19:43:00 UTC
Description	In ashmem_ioctl of ashmem.c, there is an out-of-bounds write due to insufficient locking when accessing asma. This could

Risk And Classification

Problem Types: CWE-787

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
Google Android Bugs Let Remote Users Obtain Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracker	SECTR
Android - Inter-Process munmap due to Race Condition in ashmem - Android dos Exploit	EXPLO
Malformed Request	BID
Android Security Bulletin—January 2018 Android Open Source Project	CONFID
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)