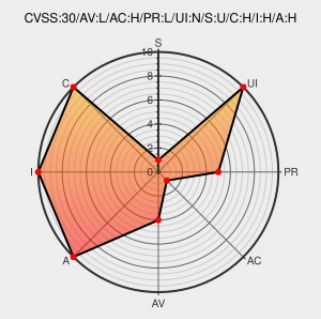
CVE-2015-9016

Published on: 04/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9016

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Android from Google contain the following vulnerability:

In blk_mq_tag_to_rq in blk-mq.c in the upstream kernel, there is a possible use after free due to a race condition when a request has been previously freed by blk_mq_complete_request. This could lead to local escalation of privilege. Product: Android. Versions: Android kernel. Android ID: A-63083046.

CVE-2015-9016 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google Inc.** - **Android** version **Android kernel**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Debian -- Security Information --	www.debian.org	DEBIAN DSA-4187

DSA-4187-1 linux	Depreciated Link text/html	
Android Security Bulletin—February 2018 | Android Open Source Project	Patch Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2018-02-01
blk-mq: fix race between timeout and freeing request · torvalds/linux@0048b48 · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/0048b4837affd153897ed1222283492070027aa9

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
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→