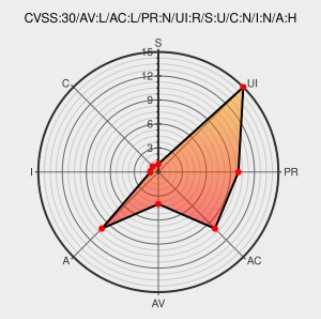
CVE-2014-9798

Published on: 07/10/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9798

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



Certain versions of Android from Google contain the following vulnerability:

platform/msm_shared/dev_tree.c in the Qualcomm bootloader in Android before 2016-07-05 on Nexus 5 devices does not check the relationship between tags addresses and aboot addresses, which allows attackers to cause a denial of service (OS outage) via a crafted application, aka Android internal bug 28821448 and Qualcomm internal bug CR681965.

CVE-2014-9798 has been assigned by security@android.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 7.1 - HIGH

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

CVE References

Description	Tags	Link
Android Security Bulletin—July 2016 | Android Open Source Project	Vendor Advisory source.android.com	CONFIRM source.android.com/security/bulletin/2016-07-01.html

	text/html	
kernel/lk -	source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/kernel/lk/commit/?id=b05eed2491a098bf627ac485a5b43d2f4fae2484

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	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→