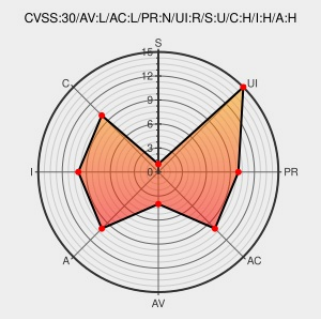
CVE-2014-9799

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

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

CVE-2014-9799

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



Certain versions of Android from Google contain the following vulnerability:

The makefile in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices omits the -fno-strict-overflow option to gcc, which might allow attackers to gain privileges via a crafted application that leverages incorrect compiler optimization of an integer-overflow protection mechanism, aka Android internal bug 28821731 and Qualcomm internal bug CR691916.

CVE-2014-9799 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
Google Nexus Qualcomm Components Multiple Privilege Escalation Vulnerabilities	cve.report (archive) text/html	BID 91628

Android Security Bulletin—July 2016 | Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-07-01.html
kernel/lk -	source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/kernel/lk/commit/?id=c2119f1fba46f3b6e153aa018f15ee46fe6d5b76

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→