



CVE-2014-9870

Published on: 08/06/2016 12:00:00 AM UTC

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

CVE-2014-9870

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

The Linux kernel before 3.11 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly consider user-space access to the TPIDRURW register, which allows local users to gain privileges via a crafted application, aka Android internal bug 28749743 and Qualcomm internal bug CR561044.

CVE-2014-9870 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
ARM: 7735/2: Preserve the user r/w register TPIDRURW on context switc... torvalds/linux@4780adeefd042482f624f5e0d577bf9cdcbb760	Issue Tracking Patch github.com	CONFIRM github.com/torvalds/linux/commit/a4780adeefd042482f624f5e0d577bf9cdcbb760

torvalds/linux@a4780ade · GitHub	text/html	
Google Nexus Qualcomm Components Multiple Privilege Escalation Vulnerabilities	cve.report (archive) text/html	 BID 92219
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch git.kernel.org text/html	 CONFIRM git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=a4780adeefd042482f624f5e0d577bf9cdccb760
kernel/msm - Kernel Tree for MSM/QSD family and Android on MSM/QSD	Issue Tracking Patch source.codeaurora.org text/html	 CONFIRM source.codeaurora.org/quic/la/kernel/msm/commit/?id=4f57652fcd2dce7741f1ac6dc0417e2f265cd1de
Android Security Bulletin—August 2016 Android Open Source Project	Vendor Advisory source.android.com text/html	 CONFIRM source.android.com/security/bulletin/2016-08-01.html

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
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:google:android:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						

No vendor comments have been submitted for this CVE