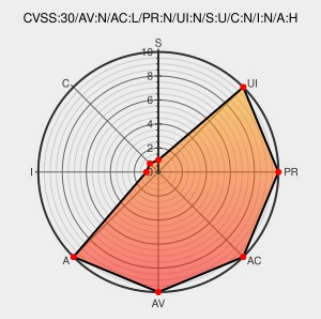
CVE-2014-9901

Published on: 08/05/2016 12:00:00 AM UTC

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

CVE-2014-9901

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



Certain versions of Android from Google contain the following vulnerability:

The Qualcomm Wi-Fi driver in Android before 2016-08-05 on Nexus 7 (2013) devices makes incorrect snprintf calls, which allows remote attackers to cause a denial of service (device hang or reboot) via crafted frames, aka Android internal bug 28670333 and Qualcomm internal bug CR548711.

CVE-2014-9901 has been assigned by security@android.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Google Nexus Qualcomm Wi-Fi Driver CVE-2014-9901 Denial of Service Vulnerability	cve.report (archive) text/html	BID 92247
Android Security Bulletin—August 2016 |	Vendor Advisory	CONFIRM source.android.com/security/bulletin/2016-08-01.html

Android Open Source Project	Vendor Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-08-01.html
platform/vendor/qcom-opensource/wlan/prima -	Issue Tracking Patch source.codeaurora.org text/html	CONFIRM source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/prima/commit/?id=637f0f7931dd7265ac1c250dc2884d6389c66bde

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→