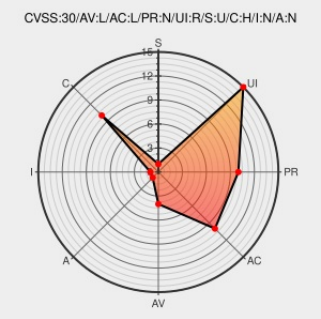
CVE-2015-8944

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

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8944

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



Certain versions of Android from Google contain the following vulnerability:

The ioresources_init function in kernel/resource.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices, uses weak permissions for /proc/iomem, which allows local users to obtain sensitive information by reading this file, aka Android internal bug 28814213 and Qualcomm internal bug CR786116. NOTE: the permissions may be intentional in most non-Android contexts.

CVE-2015-8944 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	HIGH	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
kernel/msm-3.10 - Unnamed repository	Issue Tracking Patch	CONFIRM source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?

	source.codeaurora.org text/html	id=e758417e7c31b975c862aa55d0ceef28f3cc9104
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
Google Android Qualcomm Components Multiple Information Disclosure Vulnerabilities	cve.report (archive) text/html	BID 92222
kernel-hardening - Re: [PATCH] KERNEL: resource: Fix bug on leakage in /proc/iomem file	Mailing List Third Party Advisory VDB Entry www.openwall.com text/html	MLIST [kernel-hardening] 20160406 Re: [PATCH] KERNEL: resource: Fix bug on leakage in /proc/iomem file

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

← Previous ID

Next ID→