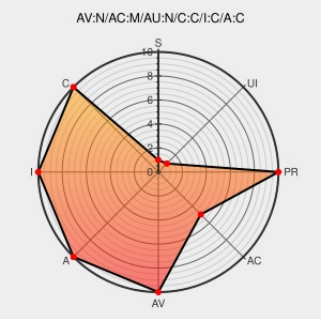
CVE-2015-3858

Published on: 09/30/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:08 PM UTC

CVE-2015-3858

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



Certain versions of Android from Google contain the following vulnerability:

The checkDestination function in internal/telephony/SMSDispatcher.java in Android before 5.1.1 LMY48M relies on an obsolete permission name for an authorization check, which allows attackers to bypass an intended user-confirmation requirement for SMS short-code messaging via a crafted application, aka internal bug 22314646.

CVE-2015-3858 has been assigned by security@android.com to track the vulnerability

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
Android Open Source Project = Details	Vendor Advisory, groups.google.com, text/plain, Inactive Link, Not Archived	MLIST [android-security-updates] 20150909 Nexus Securi
df31d37d285dde9911b699837c351aed2320b586 - platform/frameworks/opt/telephony - Git at Google	Vendor Advisory, android.googlesource.com, text/html	CONFIRM android.googlesource.com/platform/frameworks/opt/telephony

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→