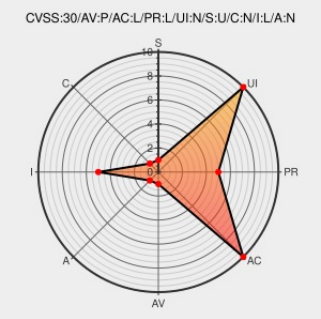
CVE-2016-3888

Published on: 09/11/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:02 PM UTC

CVE-2016-3888

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



Certain versions of Android from Google contain the following vulnerability:

internal/telephony/SMSDispatcher.java in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-09-01, and 7.0 before 2016-09-01 allows physically proximate attackers to bypass the Factory Reset Protection protection mechanism, and send premium SMS messages during the Setup Wizard provisioning stage, via unspecified vectors, aka internal bug 29420123.

CVE-2016-3888 has been assigned by security@android.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 2.1 - LOW

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Android Security Bulletin—September 2016 | Android Open Source Project	Vendor Advisory source.android.com	CONFIRM source.android.com/security/bulletin/2016-09-01.h

	text/html	
b8d1aee993dcc565e6576b2f2439a8f5a507cff6 - platform/frameworks/opt/telephony - Git at Google	Issue Tracking Patch android.googlesource.com text/html	CONFIRM android.googlesource.com/platform/frameworks/opt/telephony/+/
Google Android Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code and Let Applications Obtain Potentially Sensitive Information and Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036763
Malformed Request	cve.report (archive) text/html	BID 92857

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	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All

Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All
Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.1.2	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	4.2.1	All	All	All
Operating System	Google	Android	4.2.2	All	All	All
Operating System	Google	Android	4.3	All	All	All
Operating System	Google	Android	4.3.1	All	All	All
Operating System	Google	Android	4.4	All	All	All

Operating System	Google	Android	4.4	All	All	All
Operating System	Google	Android	4.4.1	All	All	All
Operating System	Google	Android	4.4.2	All	All	All
Operating System	Google	Android	4.4.3	All	All	All
Operating System	Google	Android	5.0	All	All	All
Operating System	Google	Android	5.0.1	All	All	All
Operating System	Google	Android	5.1	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All

cpe:2.3:o:google:android:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.0.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:5.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:6.0.1:*:*:*:*:*:*:*:

cpe:2.3:o:google:android:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report