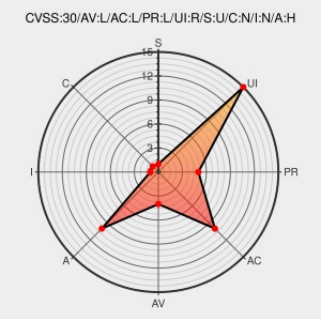
CVE-2015-6645

Published on: 01/06/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:16 PM UTC

CVE-2015-6645

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



Certain versions of Android from Google contain the following vulnerability:

SyncManager in Android before 5.1.1 LMY49F and 6.0 before 2016-01-01 allows attackers to cause a denial of service (continuous rebooting) via a crafted application, aka internal bug 23591205.

CVE-2015-6645 has been assigned by security@android.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5 - MEDIUM

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

CVSS2 Score: 7.1 - HIGH

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

CVE References

Description	Tags	Link
Nexus Security Bulletin - January 2016 | Android Open Source Project	Vendor Advisory, source.android.com, text/html	CONFIRM source.android.com/security/bulletin/2016-01-01.html
Google Android Multiple Flaws Let Remote Users Execute Arbitrary	www.securitytracker.com	SECTRACK 1034592

Code and Applications Gain Elevated Privileges - SecurityTracker text/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	4.4.4	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	5.0.2	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	4.4.4	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	5.0.2	All	All	All
Operating System	Google	Android	5.1.0	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All

cpe:2.3:o:google:android:4.4.4:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:5.0.2:*:*:*:*:*:*:*:

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

cpe:2.3:o:google:android:5.1.1:*:*:*:*:*:*:*:

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

cpe:2.3:o:google:android:4.4.4:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:google:android:5.0.2:*:*:*:*:*:*:*:

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

cpe:2.3:o:google:android:5.1.1:*:*:*:*:*:*:*:

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

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