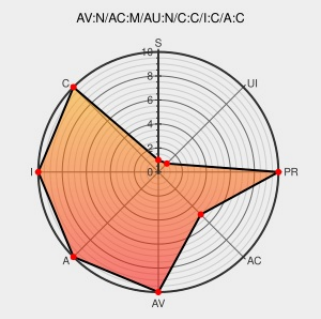
CVE-2015-3837

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

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

CVE-2015-3837

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



Certain versions of Android from Google contain the following vulnerability:

The OpenSSLX509Certificate class in org/conscrypt/OpenSSLX509Certificate.java in Android before 5.1.1 LMY48I improperly includes certain context data during serialization and deserialization, which allows attackers to execute arbitrary code via an application that sends a crafted Intent, aka internal bug 21437603.

CVE-2015-3837 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
edf7055461e2d7fa18de5196dca80896a56e3540 - platform/external/conscrypt - Git at Google	Vendor Advisory, android.googlesource.com, text/html	CONFIRM android.googlesource.com/platform/external/conscrypt/+/edf7(
	Vendor Advisory, groups.google.com, text/plain, Inactive Link, Not Archived	MLIST [android-security-updates] 20150812 Nexus Securit

comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Demo for CVE-2015-3837.

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→