



CVE-2013-7372

Published on: 04/29/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

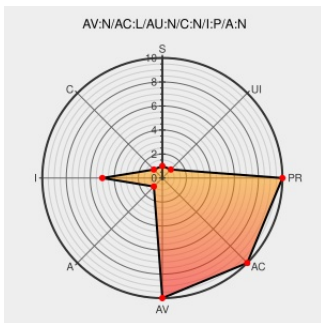
CVE-2013-7372

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Harmony](#) from [Apache](#) contain the following vulnerability:

The engineNextBytes function in

classlib/modules/security/src/main/java/common/org/apache/harmony/security/provider/crypto/ in the SecureRandom implementation in Apache Harmony through 6.0M3, as used in the Java Cryptography Architecture (JCA) in Android before 4.4 and other products, when no seed is provided by the user, uses an incorrect offset value, which makes it easier for attackers to defeat cryptographic protection mechanisms by leveraging the resulting PRNG predictability, as exploited in the wild against Bitcoin wallet applications in August 2013.

CVE-2013-7372 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

luni/src/main/java/org/apache/harmony/security/provider/crypto/SHA1PRNG_SecureRandomImpl.java - platform/libcore - Git at Google

Tags

[Patch](#)
[android.googlesource.com](#)
[text/html](#)

Some SecureRandom Thoughts | Android Developers Blog

[Patch](#)
[android-developers.blogspot.com.au](#)

[text/html](#)[Exploit](#)[www.nds.rub.de](#)[application/pdf](#)

Android Security Vulnerability

[bitcoin.org](#)[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
Application	Apache	Harmony	All	m3	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	4.0	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	All	All	All	All
cpe:2.3:a:apache:harmony:*:m3:*:*:*:*:						
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:4.0:*:*:*:*:*:						
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:*****:

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 registered 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](#)