



CVE-2015-1528

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

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-1528

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Android](#) from [Google](#) contain the following vulnerability:

Integer overflow in the native_handle_create function in libcutils/native_handle.c in Android before 5.1.1 LMY48M allows attackers to obtain a different application's privileges or cause a denial of service (Binder heap memory corruption) via a crafted application, aka internal bug 19334482.

CVE-2015-1528 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

[www.blackhat.com](#)
[application/pdf](#)

MISC [www.blackhat.com/docs/us-15/materials/us-15-Gong-Binder-Call-To-Escalate-Privilege.pdf](#)

e8c62fb484151f76ab88b1d5130f38de24ac8c14
- platform/system/core - Git at Google

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

CONFIRM
[android.googlesource.com/platform/system/core/+e8c62fb484](#)

7dcd0ec9c91688cfa3f679804ba6e132f9811254
- platform/frameworks/native - Git at Google

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

CONFIRM
[android.googlesource.com/platform/frameworks/native/+7dcd0ec9c91688cfa3f679804ba6e132f9811254](#)

Android Open Source Project = Details

[Vendor Advisory](#)
[groups.google.com](#)
[text/plain](#)
[Inactive Link](#) [Not Archived](#)

MLIST [[android-security-updates](#)] 20150909 Nexus Security

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	All	All	All	All
cpe:2.3:o:google:android:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→