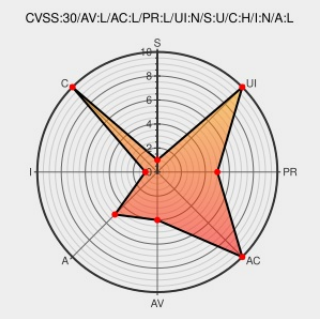
CVE-2015-8956

Published on: 10/10/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8956

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



Certain versions of Android from Google contain the following vulnerability:

The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket.

CVE-2015-8956 has been assigned by security@android.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2016:2574
Android Security Bulletin—	Patch	CONFIRM source.android.com/security/bulletin/2016-10-01.html

October 2016 | Android Open Source Project	Vendor Advisory source.android.com text/html	
Google Android Multiple Kernel Components Multiple Information Disclosure Vulnerabilites	cve.report (archive) text/html	BID 93326
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=951b6a0717db97ce420547222647bcc40bf1eacd
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2584
Bluetooth: Fix potential NULL dereference in RFCOMM bind callback · torvalds/linux@951b6a0 · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/951b6a0717db97ce420547222647bcc40bf1eacd

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
Operating System	Linux	Linux Kernel	All	All	All	All

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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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