

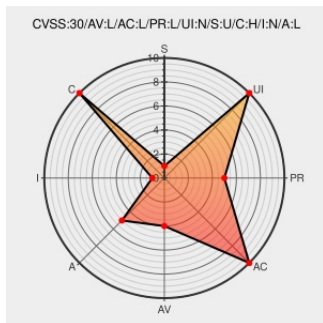


# CVE-2015-8956

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](mailto: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    | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br><b>Inactive Link</b> <b>Not Archived</b> | <a href="#">REDHAT RHSA-2016:2574</a>                                        |
| Android Security Bulletin— | <a href="#">Patch</a>                                                                                    | <a href="#">CONFIRM source.android.com/security/bulletin/2016-10-01.html</a> |

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

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](mailto: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                                 | <a href="#">Google</a> | <a href="#">Android</a>      | All     | All    | All     | All      |
| Operating System                                 | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | All     | All    | All     | All      |
| <div>cpe:2.3:o:google:android:*****:.*</div>     |                        |                              |         |        |         |          |
| <div>cpe:2.3:o:linux:linux_kernel:*****:.*</div> |                        |                              |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

