



# CVE-2015-0571

Published on: 05/09/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:18 PM UTC

## CVE-2015-0571

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

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

The WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not verify authorization for private SET IOCTL calls, which allows attackers to gain privileges via a crafted application, related to wlan\_hdd\_hostapd.c and wlan\_hdd\_wext.c.

CVE-2015-0571 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **9.3 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                      | Tags                                                                                               | Link                                                                                            |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Android Security Bulletin—May 2016   Android Open Source Project | <a href="#">Vendor Advisory</a><br><a href="#">source.android.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM</a><br><a href="#">source.android.com/security/bulletin/2016-05-01.html</a> |

RETIRED: Huawei Smart Phones Memory Buffer Overflow Vulnerability

Third Party Advisory

VDB Entry

cve.report (archive)

text/html

BID 77691

Multiple Issues in WLAN Driver Allow Local Privilege Escalation (CVE-2015-0569, CVE-2015-0570, CVE-2015-0571) | Code Aurora

Broken Link

web.archive.org

text/html

Inactive Link

Not Archived

CONFIRM

www.codeaurora.org/projects/security-advisories/multiple-issues-wlan-driver-allow-local-privilege-escalation-cve-2015

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 | Linux  | Linux Kernel | All     | All    | All     | All      |
| Operating System | Linux  | Linux Kernel | All     | All    | All     | All      |

cpe:2.3:o:linux:linux\_kernel:\*\*\*\*\*:

cpe:2.3:o:linux:linux\_kernel:\*\*\*\*\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →