

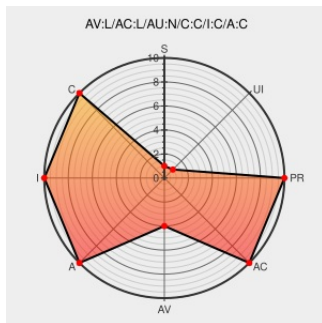


# CVE-2014-4322

Published on: 12/24/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:44 PM UTC

## CVE-2014-4322

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

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

drivers/misc/qseecom.c in the QSEECOM driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate certain offset, length, and base values within an ioctl call, which allows attackers to gain privileges or cause a denial of service (memory corruption) via a crafted application.

CVE-2014-4322 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| LOCAL                  | LOW               | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| COMPLETE               | COMPLETE          | COMPLETE            |

## CVE References

| Description                                                             | Tags                                                                                                                                                                                   | Link                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Memory corruption in QSEECOM driver (CVE-2014-4322)   Code Aurora Forum | <a href="#">Patch</a><br><a href="#">Vendor Advisory</a><br><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="#">CONFIRM</a> <a href="http://www.codeaurora.org/projects/security-advisories/memory-corruption-qseecom-driver-cve-2014-4322">www.codeaurora.org/projects/security-advisories/memory-corruption-qseecom-driver-cve-2014-4322</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

Exploit/POC from Github

Just an attempt to adapt for Note 4, I do not know what I am doing.

Known Affected Configurations (CPE V2.3)

| Type                                 | Vendor | Product      | Version | Update | Edition | Language |
|--------------------------------------|--------|--------------|---------|--------|---------|----------|
| Operating System                     | Linux  | Linux Kernel | All     | All    | All     | All      |
| cpe:2.3:o:linux:linux_kernel:*****:: |        |              |         |        |         |          |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→