



CVE-2012-4221

Published on: 11/30/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

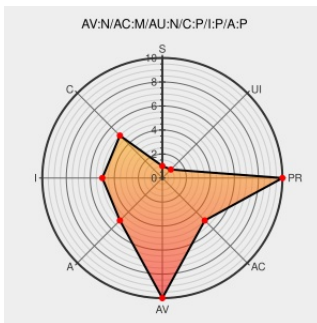
CVE-2012-4221

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Integer overflow in diagchar_core.c in the Qualcomm Innovation Center (QuIC) Diagnostics (aka DIAG) kernel-mode driver for Android 2.3 through 4.2 allows attackers to execute arbitrary code or cause a denial of service via an application that uses crafted arguments in a local diagchar_ioctl call.

CVE-2012-4221 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Vulnerability Note VU#702452 - Qualcomm Android OS kernel privilege escalation and denial of service vulnerabilities

[US Government Resource](#)
[www.kb.cert.org](#)
[text/html](#)

[CERT-VN VU#702452](#)

Multiple issues in DIAG/KGSL system call handling (CVE-2012-4220, CVE-2012-4221, CVE-2012-4222) | Code Aurora Forum

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM](#)
[www.codeaurora.org/projects/security-advisories/multiple-issues-diagkgsl-system-call-handling-cve-2012-4220-cve-2012-4221-cve-2012-4222](#)

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	2.3	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	2.3.1	All	All	All
Operating System	Google	Android	2.3.2	All	All	All
Operating System	Google	Android	2.3.3	All	All	All
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.5	All	All	All
Operating System	Google	Android	2.3.6	All	All	All
Operating System	Google	Android	2.3.7	All	All	All
Operating System	Google	Android	3.0	All	All	All
Operating System	Google	Android	3.1	All	All	All
Operating System	Google	Android	3.2	All	All	All
Operating System	Google	Android	3.2.1	All	All	All
Operating System	Google	Android	3.2.2	All	All	All
Operating System	Google	Android	3.2.4	All	All	All
Operating System	Google	Android	3.2.6	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All

Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.2	All	All	All
Operating System	Google	Android	2.3	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	2.3.1	All	All	All
Operating System	Google	Android	2.3.2	All	All	All
Operating System	Google	Android	2.3.3	All	All	All
Operating System	Google	Android	2.3.4	All	All	All
Operating System	Google	Android	2.3.5	All	All	All
Operating System	Google	Android	2.3.6	All	All	All
Operating System	Google	Android	2.3.7	All	All	All
Operating System	Google	Android	3.0	All	All	All
Operating System	Google	Android	3.1	All	All	All
Operating System	Google	Android	3.2	All	All	All
Operating System	Google	Android	3.2.1	All	All	All
Operating System	Google	Android	3.2.2	All	All	All
Operating System	Google	Android	3.2.4	All	All	All
Operating System	Google	Android	3.2.6	All	All	All
Operating System	Google	Android	4.0	All	All	All
Operating System	Google	Android	4.0.1	All	All	All
Operating System	Google	Android	4.0.2	All	All	All
Operating System	Google	Android	4.0.3	All	All	All

Operating System	Google	Android	4.0.4	All	All	All
Operating System	Google	Android	4.1	All	All	All
Operating System	Google	Android	4.2	All	All	All
cpe:2.3:o:google:android:2.3:*****:						
cpe:2.3:o:google:android:2.3:rev1:*****:						
cpe:2.3:o:google:android:2.3.1:*****:						
cpe:2.3:o:google:android:2.3.2:*****:						
cpe:2.3:o:google:android:2.3.3:*****:						
cpe:2.3:o:google:android:2.3.4:*****:						
cpe:2.3:o:google:android:2.3.5:*****:						
cpe:2.3:o:google:android:2.3.6:*****:						
cpe:2.3:o:google:android:2.3.7:*****:						
cpe:2.3:o:google:android:3.0:*****:						
cpe:2.3:o:google:android:3.1:*****:						
cpe:2.3:o:google:android:3.2:*****:						
cpe:2.3:o:google:android:3.2.1:*****:						
cpe:2.3:o:google:android:3.2.2:*****:						
cpe:2.3:o:google:android:3.2.4:*****:						
cpe:2.3:o:google:android:3.2.6:*****:						
cpe:2.3:o:google:android:4.0:*****:						
cpe:2.3:o:google:android:4.0.1:*****:						
cpe:2.3:o:google:android:4.0.2:*****:						
cpe:2.3:o:google:android:4.0.3:*****:						
cpe:2.3:o:google:android:4.0.4:*****:						
cpe:2.3:o:google:android:4.1:*****:						
cpe:2.3:o:google:android:4.2:*****:						
cpe:2.3:o:google:android:2.3:*****:						
cpe:2.3:o:google:android:2.3:rev1:*****:						

cpe:2.3:o:google:android:2.3.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:2.3.2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:2.3.3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:2.3.4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:2.3.5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:2.3.6:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:2.3.7:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.0:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.2.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.2.2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.2.4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:3.2.6:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.0:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.0.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.0.2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.0.3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.0.4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:google:android:4.2:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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