



CVE-2012-4220

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-4220
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-30 12:54:00 UTC
Updated	2013-10-10 18:28:00 UTC
Description	diagchar_core.c in the Qualcomm Innovation Center (QuIC) Diagnostics (aka DIAG) kernel-mode driver for Android 2.3 thro

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References						
Reference						Source
Vulnerability Note VU#702452 - Qualcomm Android OS kernel privilege escalation and denial of service vulnerabilites						CERT-VN
Multiple issues in DIAG/KGSL system call handling (CVE-2012-4220, CVE-2012-4221, CVE-2012-4222) Code Aurora Forum						CONFIRM
CVE Program record						CVE.ORG

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)