CVE-2010-4804

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-4804
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-09 10:36:00 UTC
Updated	2023-11-07 02:06:00 UTC
Description	The Android browser in Android before 2.3.4 allows remote attackers to obtain SD card contents via crafted content:// URIs

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	1.5	All	All	All
Operating System	Google	Android	1.6	All	All	All
Operating System	Google	Android	2.1	All	All	All
Operating System	Google	Android	2.2	All	All	All
Operating System	Google	Android	2.2	rev1	All	All
Operating System	Google	Android	2.2.1	All	All	All
Operating System	Google	Android	2.2.2	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	1.5	All	All	All
Operating System	Google	Android	1.6	All	All	All
Operating System	Google	Android	2.1	All	All	All
Operating System	Google	Android	2.2	All	All	All
Operating System	Google	Android	2.2	rev1	All	All
Operating System	Google	Android	2.2.1	All	All	All
Operating System	Google	Android	2.2.2	All	All	All
Operating System	Google	Android	2.3	rev1	All	All
Operating System	Google	Android	All	All	All	All

References

Reference	Source	Link	Tags
Open Handset Alliance Android 'content://' URI Multiple Information Disclosure Vulnerabilities	BID	www.securityfocus.com	
Android Data Stealing Vulnerability | thomascannon.net	MISC	thomascannon.net	
android.git.kernel.org		android.git.kernel.org	
android.git.kernel.org	CONFIRM	android.git.kernel.org	
android.git.kernel.org		android.git.kernel.org	
Nexus S Vulnerability	MISC	www.csc.ncsu.edu	
android.git.kernel.org	CONFIRM	android.git.kernel.org	
Android data theft exploit to be plugged in Gingerbread [Video] - SlashGear	MISC	www.slashgear.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

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