



CVE-2009-2204

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

Summary

CVE	CVE-2009-2204
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-03 18:30:00 UTC
Updated	2010-03-30 04:00:00 UTC
Description	Unspecified vulnerability in the CoreTelephony component in Apple iPhone OS before 3.0.1 allows remote attackers to ex

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	1.0	All	All	All
Operating System	Apple	Iphone Os	1.0.0	All	All	All
Operating System	Apple	Iphone Os	1.0.1	All	All	All
Operating System	Apple	Iphone Os	1.0.2	All	All	All
Operating System	Apple	Iphone Os	1.1	All	All	All
Operating System	Apple	Iphone Os	1.1.0	All	All	All
Operating System	Apple	Iphone Os	1.1.1	All	All	All
Operating System	Apple	Iphone Os	1.1.2	All	All	All
Operating System	Apple	Iphone Os	1.1.3	All	All	All
Operating System	Apple	Iphone Os	1.1.4	All	All	All
Operating System	Apple	Iphone Os	1.1.5	All	All	All
Operating System	Apple	Iphone Os	2.0	All	All	All
Operating System	Apple	Iphone Os	2.0.0	All	All	All
Operating System	Apple	Iphone Os	2.0.1	All	All	All
Operating System	Apple	Iphone Os	2.0.2	All	All	All
Operating System	Apple	Iphone Os	2.1	All	All	All
Operating System	Apple	Iphone Os	1.0	All	All	All

Operating System	Apple	Iphone Os	1.0.0	All	All	All
Operating System	Apple	Iphone Os	1.0.1	All	All	All
Operating System	Apple	Iphone Os	1.0.2	All	All	All
Operating System	Apple	Iphone Os	1.1	All	All	All
Operating System	Apple	Iphone Os	1.1.0	All	All	All
Operating System	Apple	Iphone Os	1.1.1	All	All	All
Operating System	Apple	Iphone Os	1.1.2	All	All	All
Operating System	Apple	Iphone Os	1.1.3	All	All	All
Operating System	Apple	Iphone Os	1.1.4	All	All	All
Operating System	Apple	Iphone Os	1.1.5	All	All	All
Operating System	Apple	Iphone Os	2.0	All	All	All
Operating System	Apple	Iphone Os	2.0.0	All	All	All
Operating System	Apple	Iphone Os	2.0.1	All	All	All
Operating System	Apple	Iphone Os	2.0.2	All	All	All
Operating System	Apple	Iphone Os	2.1	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All

References						
Reference				Source	Link	
55687				OSVDB	wv	
SecurityTracker.com Archives - Apple iPhone SMS Message Processing Bugs Let Remote Users Execute Arbitrary Code				SECTrack	se	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	wv	
APPLE-SA-2009-07-31-1 iPhone OS 3.0.1				APPLE	list	
Apple iPhone SMS Message Decoding Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA	se	
SyScan'10 Singapore :: Day 1 (17 June 2010)				MISC	wv	
About the security content of iPhone OS 3.0.1				CONFIRM	su	
Apple iPhone SMS Application Remote Code Execution Vulnerability				BID	wv	
www.blackhat.com/presentations/bh-usa-09/MILLER/BHUSA09-Miller-FuzzingPhone-PA...				MISC	wv	
Researcher hopes Apple fixes possible iPhone SMS security hole Security - CNET News				MISC	ne	
CVE Program record				CVE.ORG	wv	
NVD vulnerability detail				NVD	nv	

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](#)