



CVE-2009-1723

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

Summary

CVE	CVE-2009-1723
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-06 15:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	CFNetwork in Apple Mac OS X 10.5 before 10.5.8 places an incorrect URL in a certificate warning in certain 302 redirection

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Mac Os X	10.5.6	All	All	All
Operating System	Apple	Mac Os X	10.5	All	All	All
Operating System	Apple	Mac Os X	10.5.0	All	All	All
Operating System	Apple	Mac Os X	10.5.1	All	All	All
Operating System	Apple	Mac Os X	10.5.2	All	All	All
Operating System	Apple	Mac Os X	10.5.2	2008-002	All	All
Operating System	Apple	Mac Os X	10.5.3	All	All	All
Operating System	Apple	Mac Os X	10.5.4	All	All	All
Operating System	Apple	Mac Os X	10.5.5	All	All	All
Operating System	Apple	Mac Os X	10.5.6	All	All	All
Operating System	Apple	Mac Os X	10.5.7	All	All	All
Application	Apple	Mac Os X	10.5.6	All	All	All
Operating System	Apple	Mac Os X	10.5	All	All	All
Operating System	Apple	Mac Os X	10.5.0	All	All	All
Operating System	Apple	Mac Os X	10.5.1	All	All	All
Operating System	Apple	Mac Os X	10.5.2	All	All	All
Operating System	Apple	Mac Os X	10.5.2	2008-002	All	All

Operating System	Apple	Mac Os X	10.5.3	All	All	All
Operating System	Apple	Mac Os X	10.5.4	All	All	All
Operating System	Apple	Mac Os X	10.5.5	All	All	All
Operating System	Apple	Mac Os X	10.5.6	All	All	All
Operating System	Apple	Mac Os X	10.5.7	All	All	All
Operating System	Apple	Mac Os X Server	10.5	All	All	All
Operating System	Apple	Mac Os X Server	10.5.0	All	All	All
Operating System	Apple	Mac Os X Server	10.5.1	All	All	All
Operating System	Apple	Mac Os X Server	10.5.2	All	All	All
Operating System	Apple	Mac Os X Server	10.5.3	All	All	All
Operating System	Apple	Mac Os X Server	10.5.4	All	All	All
Operating System	Apple	Mac Os X Server	10.5.5	All	All	All
Operating System	Apple	Mac Os X Server	10.5.6	All	All	All
Operating System	Apple	Mac Os X Server	10.5.7	All	All	All
Operating System	Apple	Mac Os X Server	10.5	All	All	All
Operating System	Apple	Mac Os X Server	10.5.0	All	All	All
Operating System	Apple	Mac Os X Server	10.5.1	All	All	All
Operating System	Apple	Mac Os X Server	10.5.2	All	All	All
Operating System	Apple	Mac Os X Server	10.5.3	All	All	All
Operating System	Apple	Mac Os X Server	10.5.4	All	All	All
Operating System	Apple	Mac Os X Server	10.5.5	All	All	All
Operating System	Apple	Mac Os X Server	10.5.6	All	All	All
Operating System	Apple	Mac Os X Server	10.5.7	All	All	All

References						
Reference	Source		Impact			
Apple Mac OS X 2009-003 Multiple Security Vulnerabilities	BID		Low	Medium	High	Very High
56846	OSVDB		Low	Medium	High	Very High
About the security content of iOS 4	CONFIRM		Low	Medium	High	Very High
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA		Low	Medium	High	Very High
APPLE-SA-2010-06-21-1 iOS 4	APPLE		Low	Medium	High	Very High
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN		Low	Medium	High	Very High
About the security content of Security Update 2009-003 / Mac OS X v10.5.8	CONFIRM		Low	Medium	High	Very High
IBM X-Force Exchange	XF		Low	Medium	High	Very High
US-CERT Technical Cyber Security Alert TA09-218A -- Apple Updates for Multiple Vulnerabilities	CERT		Low	Medium	High	Very High
APPLE-SA-2009-06-25-1 OS X v10.5.7, OS X v10.5.8, OS X v10.5.9, OS X v10.5.10, OS X v10.5.11, OS X v10.5.12, OS X v10.5.13, OS X v10.5.14, OS X v10.5.15, OS X v10.5.16, OS X v10.5.17, OS X v10.5.18, OS X v10.5.19, OS X v10.5.20, OS X v10.5.21, OS X v10.5.22, OS X v10.5.23, OS X v10.5.24, OS X v10.5.25, OS X v10.5.26, OS X v10.5.27, OS X v10.5.28, OS X v10.5.29, OS X v10.5.30, OS X v10.5.31, OS X v10.5.32, OS X v10.5.33, OS X v10.5.34, OS X v10.5.35, OS X v10.5.36, OS X v10.5.37, OS X v10.5.38, OS X v10.5.39, OS X v10.5.40, OS X v10.5.41, OS X v10.5.42, OS X v10.5.43, OS X v10.5.44, OS X v10.5.45, OS X v10.5.46, OS X v10.5.47, OS X v10.5.48, OS X v10.5.49, OS X v10.5.50, OS X v10.5.51, OS X v10.5.52, OS X v10.5.53, OS X v10.5.54, OS X v10.5.55, OS X v10.5.56, OS X v10.5.57, OS X v10.5.58, OS X v10.5.59, OS X v10.5.60, OS X v10.5.61, OS X v10.5.62, OS X v10.5.63, OS X v10.5.64, OS X v10.5.65, OS X v10.5.66, OS X v10.5.67, OS X v10.5.68, OS X v10.5.69, OS X v10.5.70, OS X v10.5.71, OS X v10.5.72, OS X v10.5.73, OS X v10.5.74, OS X v10.5.75, OS X v10.5.76, OS X v10.5.77, OS X v10.5.78, OS X v10.5.79, OS X v10.5.80, OS X v10.5.81, OS X v10.5.82, OS X v10.5.83, OS X v10.5.84, OS X v10.5.85, OS X v10.5.86, OS X v10.5.87, OS X v10.5.88, OS X v10.5.89, OS X v10.5.90, OS X v10.5.91, OS X v10.5.92, OS X v10.5.93, OS X v10.5.94, OS X v10.5.95, OS X v10.5.96, OS X v10.5.97, OS X v10.5.98, OS X v10.5.99, OS X v10.5.100	APPLE		Low	Medium	High	Very High

APPLE-SA-2009-08-05-1 Security Update 2009-003 / Mac OS X v10.5.8	APPLE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
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](#)