



CVE-2008-1025

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

Summary

CVE	CVE-2008-1025
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-17 19:05:00 UTC
Updated	2017-08-08 01:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Apple WebKit, as used in Safari before 3.1.1, allows remote attackers to inject art

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	0.8	All	All	All
Application	Apple	Safari	0.9	All	All	All
Application	Apple	Safari	1.0	All	All	All
Application	Apple	Safari	1.0.3	All	All	All
Application	Apple	Safari	1.1	All	All	All
Application	Apple	Safari	1.2	All	All	All
Application	Apple	Safari	1.3	All	All	All
Application	Apple	Safari	1.3.1	All	All	All
Application	Apple	Safari	1.3.2	All	All	All
Application	Apple	Safari	2.0	All	All	All
Application	Apple	Safari	2.0.2	All	All	All
Application	Apple	Safari	2.0.4	All	All	All
Application	Apple	Safari	3.0	All	All	All
Application	Apple	Safari	3.0.2	All	All	All
Application	Apple	Safari	3.0.3	All	All	All
Application	Apple	Safari	3.0.4	All	All	All
Application	Apple	Safari	3.1	All	All	All

Application	Apple	Safari	0.8	All	All	All
Application	Apple	Safari	0.9	All	All	All
Application	Apple	Safari	1.0	All	All	All
Application	Apple	Safari	1.0.3	All	All	All
Application	Apple	Safari	1.1	All	All	All
Application	Apple	Safari	1.2	All	All	All
Application	Apple	Safari	1.3	All	All	All
Application	Apple	Safari	1.3.1	All	All	All
Application	Apple	Safari	1.3.2	All	All	All
Application	Apple	Safari	2.0	All	All	All
Application	Apple	Safari	2.0.2	All	All	All
Application	Apple	Safari	2.0.4	All	All	All
Application	Apple	Safari	3.0	All	All	All
Application	Apple	Safari	3.0.2	All	All	All
Application	Apple	Safari	3.0.3	All	All	All
Application	Apple	Safari	3.0.4	All	All	All
Application	Apple	Safari	3.1	All	All	All
Application	Apple	Webkit	All	All	All	All
Application	Apple	Webkit	All	All	All	All

References						
Reference				Source	Link	
Apple iPhone / iPod touch Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA	secunia.com	
Safari WebKit Input Validation Bug in Processing URLs Permits Cross-Site Scripting Attacks - SecurityTracker				SECTRACK	www.securiti	
Webmail - OVH				VUPEN	www.vupen	
About the security content of Safari 3.1.1				CONFIRM	support.app	
Apple Safari WebKit URI Handling Cross-Site Scripting Vulnerability				BID	www.securiti	
Safari Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA	secunia.com	
APPLE-SA-2008-07-11 iPhone 2.0 and iPod touch 2.0				APPLE	lists.apple.c	
IBM X-Force Exchange				XF	exchange.xf	
APPLE-SA-2008-04-16 Safari 3.1.1				APPLE	lists.apple.c	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen	
US-CERT Vulnerability Note VU#705529				CERT-VN	www.kb.cer	
CVE Program record				CVE.ORG	www.cve.or	
NVD vulnerability detail				NVD	nvd.nist.gov	

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](#)