

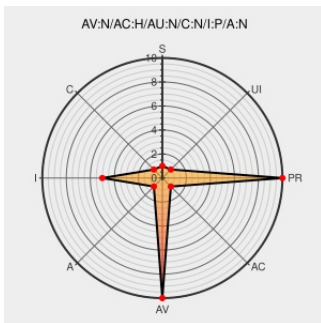


CVE-2005-2272

Published on: 07/13/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2272

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Safari](#) from [Apple](#) contain the following vulnerability:

Safari version 2.0 (412) does not clearly associate a Javascript dialog box with the web page that generated it, which allows remote attackers to spoof a dialog box from a trusted site and facilitates phishing attacks, aka the "Dialog Origin Spoofing Vulnerability."

CVE-2005-2272 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.6 - LOW**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

About Secunia Research | Flexera

[Exploit](#)
[Vendor Advisory](#)
[secunia.com](#)
[Deprecated Link](#)
[text/plain](#)

[X](#) MISC [secunia.com/secunia_research/2005-12/advisory/](#)

About Security Update 2005-009

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[🌐](#) APPLE [APPLE-SA-2005-11-29](#)

Secunia - Advisories - Mac OS X Security Update Fixes Multiple Vulnerabilities

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 17813

Secunia - Multiple Browsers Dialog Origin Vulnerability Test

[Exploit](#)
[web.archive.org](#)
[text/html](#)

[X](#) MISC [secunia.com/multiple_browsers_dialog_origin_vulnerability_test/](#)

Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-2659
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 17397
Apple Safari Dialog Box Origin Spoofing Vulnerability	cve.report (archive) text/html	BID 14011
SecurityTracker.com Archives - Apple Safari WebKit Buffer Overflow May Let Remote Users Execute Arbitrary Code and Other Bugs May Permit JavaScript Dialog Box Spoofing and File Download Location Modification	securitytracker.com text/html	SECTrack 1015294
Secunia - Advisories - Safari Dialog Origin Spoofing Vulnerability	web.archive.org text/html	SECUNIA 15474
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mozilla-javascript-dialog-box-spoofing(21070)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	2.0	All	All	All
Application	Apple	Safari	2.0	All	All	All
cpe:2.3:a:apple:safari:2.0:*:*:*:*:*:						
cpe:2.3:a:apple:safari:2.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

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](#).

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