



CVE-2011-3443

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

Summary

CVE	CVE-2011-3443
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-02 00:55:02 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Use-after-free vulnerability in WebKit, as used in Apple Safari before 5.0.6, allows remote attackers to execute arbitrary code

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	1.0	All	All	All

Application	Apple	Safari	1.0	beta	All	All
Application	Apple	Safari	1.0	beta2	All	All
Application	Apple	Safari	1.0.0	All	All	All
Application	Apple	Safari	1.0.0b1	All	All	All
Application	Apple	Safari	1.0.0b2	All	All	All
Application	Apple	Safari	1.0.1	All	All	All
Application	Apple	Safari	1.0.2	All	All	All
Application	Apple	Safari	1.0.3	All	All	All
Application	Apple	Safari	1.0.3	85.8	All	All
Application	Apple	Safari	1.0.3	85.8.1	All	All
Application	Apple	Safari	1.0b1	-	mac	All
Application	Apple	Safari	1.1	All	All	All
Application	Apple	Safari	1.1.0	All	All	All
Application	Apple	Safari	1.1.1	All	All	All
Application	Apple	Safari	1.2	All	All	All
Application	Apple	Safari	1.2.0	All	All	All
Application	Apple	Safari	1.2.1	All	All	All
Application	Apple	Safari	1.2.2	All	All	All
Application	Apple	Safari	1.2.3	All	All	All
Application	Apple	Safari	1.2.4	All	All	All
Application	Apple	Safari	1.2.5	All	All	All
Application	Apple	Safari	1.3	All	All	All
Application	Apple	Safari	1.3.0	All	All	All
Application	Apple	Safari	1.3.1	All	All	All
Application	Apple	Safari	1.3.2	All	All	All
Application	Apple	Safari	1.3.2	312.5	All	All
Application	Apple	Safari	1.3.2	312.6	All	All
Application	Apple	Safari	2.0	All	All	All
Application	Apple	Safari	2.0.0	All	All	All
Application	Apple	Safari	2.0.1	All	All	All
Application	Apple	Safari	2.0.2	All	All	All
Application	Apple	Safari	2.0.3	All	All	All
Application	Apple	Safari	2.0.3	417.8	All	All
Application	Apple	Safari	2.0.3	417.9	All	All
Application	Apple	Safari	2.0.3	417.9.2	All	All
Application	Apple	Safari	2.0.3	417.9.3	All	All

Application	Apple	Safari	2.0.4	All	All	All
Application	Apple	Safari	2.0.4	-	mac	All
Application	Apple	Safari	3.0	All	All	All
Application	Apple	Safari	3.0.0	All	All	All
Application	Apple	Safari	3.0.0	-	mac	All
Application	Apple	Safari	3.0.0b	All	All	All
Application	Apple	Safari	3.0.0b	-	windows	All
Application	Apple	Safari	3.0.1	All	All	All
Application	Apple	Safari	3.0.1	-	mac	All
Application	Apple	Safari	3.0.1	beta	All	All
Application	Apple	Safari	3.0.1b	All	All	All
Application	Apple	Safari	3.0.1b	-	windows	All
Application	Apple	Safari	3.0.2	All	All	All
Application	Apple	Safari	3.0.2	-	mac	All
Application	Apple	Safari	3.0.2b	All	All	All
Application	Apple	Safari	3.0.2b	-	windows	All
Application	Apple	Safari	3.0.3	All	All	All
Application	Apple	Safari	3.0.3	-	mac	All
Application	Apple	Safari	3.0.3b	All	All	All
Application	Apple	Safari	3.0.3b	-	windows	All
Application	Apple	Safari	3.0.4	All	All	All
Application	Apple	Safari	3.0.4	-	mac	All
Application	Apple	Safari	3.0.4b	All	All	All
Application	Apple	Safari	3.0.4b	-	windows	All
Application	Apple	Safari	3.1.0	All	All	All
Application	Apple	Safari	3.1.0	-	mac	All
Application	Apple	Safari	3.1.0b	All	All	All
Application	Apple	Safari	3.1.0b	-	windows	All
Application	Apple	Safari	3.1.1	All	All	All
Application	Apple	Safari	3.1.1b	-	windows	All
Application	Apple	Safari	3.1.2	All	All	All
Application	Apple	Safari	3.1.2b	-	windows	All
Application	Apple	Safari	3.2.0	All	All	All
Application	Apple	Safari	3.2.0b	-	windows	All
Application	Apple	Safari	3.2.1	All	All	All

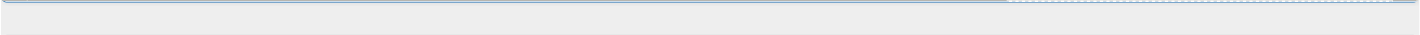
Application	Apple	Safari	3.2.1b	-	windows	All
Application	Apple	Safari	3.2.2	All	All	All
Application	Apple	Safari	3.2.2b	-	windows	All
Application	Apple	Safari	4.0	All	All	All
Application	Apple	Safari	4.0	beta	All	All
Application	Apple	Safari	4.0.0b	All	All	All
Application	Apple	Safari	4.0.1	All	All	All
Application	Apple	Safari	4.0.2	All	All	All
Application	Apple	Safari	4.0.3	All	All	All
Application	Apple	Safari	4.0.4	All	All	All
Application	Apple	Safari	4.0.5	All	All	All
Application	Apple	Safari	4.1	All	All	All
Application	Apple	Safari	4.1.1	All	All	All
Application	Apple	Safari	4.1.2	All	All	All
Application	Apple	Safari	5.0.1	All	All	All
Application	Apple	Safari	5.0.2	All	All	All
Application	Apple	Safari	5.0.3	All	All	All
Application	Apple	Safari	5.0.4	All	All	All
Application	Apple	Safari	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
About the security content of Safari 5.1 and Safari 5.0.6	af854a3a-2127-422b-91ae-364da26611
Verisign is a global provider of domain name registry services and internet infrastructure - Verisign	af854a3a-2127-422b-91ae-364da26611
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](#)