



CVE-2010-1413

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

Summary

CVE	CVE-2010-1413
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-11 18:00:40 UTC
Updated	2026-04-29 01:13:23 UTC
Description	WebKit in Apple Safari before 5.0 on Mac OS X 10.5 through 10.6 and Windows, and before 4.1 on Mac OS X 10.4, sends

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	10.5.3	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	10.5.8	All	All	All
Operating System	Apple	Mac Os X	10.6.0	All	All	All
Operating System	Apple	Mac Os X	10.6.1	All	All	All
Operating System	Apple	Mac Os X	10.6.2	All	All	All
Operating System	Apple	Mac Os X	10.6.3	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	10.5.8	All	All	All
Operating System	Apple	Mac Os X Server	10.6.0	All	All	All
Operating System	Apple	Mac Os X Server	10.6.1	All	All	All
Operating System	Apple	Mac Os X Server	10.6.2	All	All	All
Operating System	Apple	Mac Os X Server	10.6.3	All	All	All
Application	Apple	Safari	4.0	All	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	All	All	All	All
Application	Apple	Webkit	All	All	All	All
Operating System	Microsoft	Windows 7	All	All	All	All

Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All

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

References	
Reference	Score
SUSE update for Multiple Packages - Secunia.com	affected
APPLE-SA-2010-06-07-1 Safari 5.0 and Safari 4.1	affected
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	affected
About the security content of Safari 5.0 and Safari 4.1	affected
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	affected
WebKit NTLM Credentials Information Disclosure Vulnerability	affected
Repository / Oval Repository	affected
SecurityTracker.com Archives - Apple Safari Bugs Let Remote Users Execute Arbitrary Code or Access Potentially Sensitive Information	affected
About the security content of iOS 4	affected
APPLE-SA-2010-06-21-1 iOS 4	affected
RETIRED: Apple Safari Prior to 5.0 and 4.1 Multiple Security Vulnerabilities	affected
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	affected
Apple Safari Multiple Vulnerabilities - Advisories - Community	affected
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report