



CVE-2008-0894

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

Summary

CVE	CVE-2008-0894
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-02-21 21:44:00 UTC
Updated	2018-10-15 22:03:00 UTC
Description	Apple Safari might allow remote attackers to obtain potentially sensitive memory contents or cause a denial of service (cras

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

SecurityFocus

FireFox 2.0.0.11 and Opera 9.50 beta Remote Memory Information Leak, FireFox 2.0.0.11 Remote Denial of Service - SecurityReason.com

Bug 408076 – out of bounds read in BMP decoder can lead to information disclosure

Safari BMP Handling Bug Lets Remote Users Access Portions of Kernel Memory - SecurityTracker

Apple Safari BMP and GIF Files Remote Denial of Service and Information Disclosure Vulnerability

CVE Program record

NVD vulnerability detail

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](#)