



CVE-2009-2188

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

Summary

CVE	CVE-2009-2188
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-08-06 16:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Buffer overflow in ImageIO in Apple Mac OS X 10.5 before 10.5.8, and Safari before 4.0.3, allows remote attackers to execute arbitrary code via crafted PDF documents.

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Mac Os X	10.5.6	All	All	All

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	10.5.2	2008-002	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 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

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

References						
Reference						Source
US-CERT Technical Cyber Security Alert TA09-218A -- Apple Updates for Multiple Vulnerabilities						af854a3a-212
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						af854a3a-212
APPLE-SA-2009-08-11-1 Safari 4.0.3						af854a3a-212
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com						af854a3a-212
osvdb.org/56842						af854a3a-212
Apple Mac OS X 2009-003 Multiple Security Vulnerabilities						af854a3a-212
IBM X-Force Exchange						af854a3a-212
APPLE-SA-2009-08-05-1 Security Update 2009-003 / Mac OS X v10.5.8						af854a3a-212
Mac OS X Multiple Image and File Processing Bugs Permit Remote Code Execution - SecurityTracker						af854a3a-212
About the security content of Safari 4.0.3						af854a3a-212
About the security content of Security Update 2009-003 / Mac OS X v10.5.8						af854a3a-212

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](#)