



CVE-2009-0520

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

Summary

CVE	CVE-2009-0520
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-26 16:17:19 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 does not properly remove references to destroyed objects, which allows attackers to execute arbitrary code or cause a denial of service (memory consumption) via crafted SWF files.

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	Adobe	Air	1.5	All	All	All

Application	Adobe	Flash Player	10.0.0.584	All	All	All
Application	Adobe	Flash Player	10.0.12.10	All	All	All
Application	Adobe	Flash Player	7.0	All	All	All
Application	Adobe	Flash Player	7.0.1	All	All	All
Application	Adobe	Flash Player	7.0.25	All	All	All
Application	Adobe	Flash Player	7.0.63	All	All	All
Application	Adobe	Flash Player	7.0.63	All	linux	All
Application	Adobe	Flash Player	7.0.69.0	All	All	All
Application	Adobe	Flash Player	7.0.70.0	All	All	All
Application	Adobe	Flash Player	7.1	All	All	All
Application	Adobe	Flash Player	7.1.1	All	All	All
Application	Adobe	Flash Player	7.2	All	All	All
Application	Adobe	Flash Player	8.0	All	All	All
Application	Adobe	Flash Player	8.0	All	basic	All
Application	Adobe	Flash Player	8.0	All	pro	All
Application	Adobe	Flash Player	8.0.24.0	All	All	All
Application	Adobe	Flash Player	8.0.34.0	All	All	All
Application	Adobe	Flash Player	8.0.35.0	All	All	All
Application	Adobe	Flash Player	8.0.39.0	All	All	All
Application	Adobe	Flash Player	9.0.112.0	All	All	All
Application	Adobe	Flash Player	9.0.114.0	All	All	All
Application	Adobe	Flash Player	9.0.115.0	All	All	All
Application	Adobe	Flash Player	9.0.124.0	All	All	All
Application	Adobe	Flash Player	9.0.16	All	All	All
Application	Adobe	Flash Player	9.0.20	All	All	All
Application	Adobe	Flash Player	9.0.20.0	All	All	All
Application	Adobe	Flash Player	9.0.28	All	All	All
Application	Adobe	Flash Player	9.0.28.0	All	All	All
Application	Adobe	Flash Player	9.0.31.0	All	All	All
Application	Adobe	Flash Player	9.0.45.0	All	All	All
Application	Adobe	Flash Player	9.0.47.0	All	All	All
Application	Adobe	Flash Player	9.0.48.0	All	All	All
Application	Adobe	Flash Player	cs3	All	pro	All
Application	Adobe	Flash Player	cs4	All	pro	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player For Linux	All	All	All	All

Application	Adobe	Flex	3.0	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
rhn.redhat.com Red Hat Support				af854a3a-212		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-212		
Adobe flash player patch				af854a3a-212		
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7				af854a3a-212		
Bug 487142 – CVE-2009-0520 flash-plugin: Buffer overflow (arbitrary code execution) via crafted SWF file.				af854a3a-212		
Gentoo Linux Documentation -- Adobe Flash Player: Multiple vulnerabilities				af854a3a-212		
Repository / Oval Repository				af854a3a-212		
labs.iddefense.com/intelligence/vulnerabilities/display.php				af854a3a-212		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-212		
About the security content of Security Update 2009-002 / Mac OS X v10.5.7				af854a3a-212		
Adobe Flash Player Invalid Object Reference Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker				af854a3a-212		
Repository / Oval Repository				af854a3a-212		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-212		
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com				af854a3a-212		
Adobe Flash Player Invalid Object Reference Remote Code Execution Vulnerability				af854a3a-212		
IBM X-Force Exchange				af854a3a-212		
rhn.redhat.com Red Hat Support				af854a3a-212		
Adobe - Security Advisories : APSB09-01 - Flash Player update available to address security vulnerabilities				af854a3a-212		
Adobe Flash Player Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com				af854a3a-212		
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities				af854a3a-212		
#254909: Multiple Security Vulnerabilities in the Adobe Flash Player for Solaris 10 (Adobe Security Bulletin APSB09-01)				af854a3a-212		
Sun Solaris Adobe Flash Player Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com				af854a3a-212		
Gentoo update for netscape-flash - Secunia Advisories - Vulnerability Information - Secunia.com				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](#)