



CVE-2010-2185

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

Summary

CVE	CVE-2010-2185
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-15 18:00:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	Buffer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, mi

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Air	1.0	All	All	All
Application	Adobe	Air	1.1	All	All	All
Application	Adobe	Air	1.5	All	All	All
Application	Adobe	Air	1.5.1	All	All	All
Application	Adobe	Air	1.5.2	All	All	All
Application	Adobe	Air	1.5.3	All	All	All
Application	Adobe	Air	1.0	All	All	All
Application	Adobe	Air	1.1	All	All	All
Application	Adobe	Air	1.5	All	All	All
Application	Adobe	Air	1.5.1	All	All	All
Application	Adobe	Air	1.5.2	All	All	All
Application	Adobe	Air	1.5.3	All	All	All
Application	Adobe	Air	All	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	10.0.12.36	All	All	All
Application	Adobe	Flash Player	10.0.15.3	All	All	All

Application	Adobe	Flash Player	10.0.22.87	All	All	All
Application	Adobe	Flash Player	10.0.32.18	All	All	All
Application	Adobe	Flash Player	10.0.42.34	All	All	All
Application	Adobe	Flash Player	6.0.79	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	7.0.14.0	All	All	All
Application	Adobe	Flash Player	7.0.19.0	All	All	All
Application	Adobe	Flash Player	7.0.24.0	All	All	All
Application	Adobe	Flash Player	7.0.25	All	All	All
Application	Adobe	Flash Player	7.0.53.0	All	All	All
Application	Adobe	Flash Player	7.0.60.0	All	All	All
Application	Adobe	Flash Player	7.0.61.0	All	All	All
Application	Adobe	Flash Player	7.0.63	All	All	All
Application	Adobe	Flash Player	7.0.66.0	All	All	All
Application	Adobe	Flash Player	7.0.67.0	All	All	All
Application	Adobe	Flash Player	7.0.68.0	All	All	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	7.0.73.0	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	8.0.22.0	All	All	All
Application	Adobe	Flash Player	8.0.24.0	All	All	All
Application	Adobe	Flash Player	8.0.33.0	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	8.0.42.0	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	9.0.125.0	All	All	All
Application	Adobe	Flash Player	9.0.151.0	All	All	All

Application	Adobe	Flash Player	9.0.152.0	All	All	All
Application	Adobe	Flash Player	9.0.159.0	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	9.0.246.0	All	All	All
Application	Adobe	Flash Player	9.0.260.0	All	All	All
Application	Adobe	Flash Player	9.0.262.0	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	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	10.0.0.584	All	All	All
Application	Adobe	Flash Player	10.0.12.10	All	All	All
Application	Adobe	Flash Player	10.0.12.36	All	All	All
Application	Adobe	Flash Player	10.0.15.3	All	All	All
Application	Adobe	Flash Player	10.0.22.87	All	All	All
Application	Adobe	Flash Player	10.0.32.18	All	All	All
Application	Adobe	Flash Player	10.0.42.34	All	All	All
Application	Adobe	Flash Player	6.0.79	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	7.0.14.0	All	All	All
Application	Adobe	Flash Player	7.0.19.0	All	All	All
Application	Adobe	Flash Player	7.0.24.0	All	All	All
Application	Adobe	Flash Player	7.0.25	All	All	All
Application	Adobe	Flash Player	7.0.53.0	All	All	All
Application	Adobe	Flash Player	7.0.60.0	All	All	All
Application	Adobe	Flash Player	7.0.61.0	All	All	All
Application	Adobe	Flash Player	7.0.63	All	All	All
Application	Adobe	Flash Player	7.0.66.0	All	All	All
Application	Adobe	Flash Player	7.0.67.0	All	All	All
Application	Adobe	Flash Player	7.0.68.0	All	All	All

Application	Adobe	Flash Player	7.0.68.0	All	All	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	7.0.73.0	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	8.0.22.0	All	All	All
Application	Adobe	Flash Player	8.0.24.0	All	All	All
Application	Adobe	Flash Player	8.0.33.0	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	8.0.42.0	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	9.0.125.0	All	All	All
Application	Adobe	Flash Player	9.0.151.0	All	All	All
Application	Adobe	Flash Player	9.0.152.0	All	All	All
Application	Adobe	Flash Player	9.0.159.0	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	9.0.246.0	All	All	All
Application	Adobe	Flash Player	9.0.260.0	All	All	All
Application	Adobe	Flash Player	9.0.262.0	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	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	All	All	All	All
Application	Macromedia	Flash Player	5.0	All	All	All

Application	Macromedia	Flash Player	5.0.30.0	All	All	All
Application	Macromedia	Flash Player	5.0.41.0	All	All	All
Application	Macromedia	Flash Player	5.0.42.0	All	All	All
Application	Macromedia	Flash Player	5.0.58.0	All	All	All
Application	Macromedia	Flash Player	5.0	All	All	All
Application	Macromedia	Flash Player	5.0.30.0	All	All	All
Application	Macromedia	Flash Player	5.0.41.0	All	All	All
Application	Macromedia	Flash Player	5.0.42.0	All	All	All
Application	Macromedia	Flash Player	5.0.58.0	All	All	All

References

Reference

404 Not Found

[rhnl.redhat.com | Red Hat Support](#)

[Repository / Oval Repository](#)

[APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007](#)

[Gentoo update for adobe-flash - Advisories - Community](#)

[Adobe AIR Multiple Vulnerabilities - Advisories - Community](#)

[US-CERT Technical Cyber Security Alert TA10-162A -- Adobe Flash and AIR Vulnerabilities](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[SSRT100179](#)

[RETIRED: Adobe Flash Player 10.0.45.2 and AIR 1.5.3.9130 Multiple Remote Vulnerabilities](#)

[rhnl.redhat.com | Red Hat Support](#)

[IBM X-Force Exchange](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Repository / Oval Repository](#)

[HP Systems Insight Manager Multiple Vulnerabilities - Advisories - Community](#)

[\[security-announce\] SUSE Security Announcement: flash player \(SUSE-SA:20](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[SecurityTracker.com Archives - Adobe Flash Player Multiple Flaws Let Remote Users Execute Arbitrary Code, Conduct Cross-Site Scripting At](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[Gentoo Linux Documentation -- Adobe Flash Player: Multiple vulnerabilities](#)

[\[security-announce\] SUSE Security Summary Report: SUSE-SR:2010:013](#)

[Adobe Security Bulletin: APSB10-14 Security update available for Adobe Flash Player](#)

Adobe - Security Bulletins: AFSB10-14 Security update available for Adobe Flash Player

SecurityTracker.com Archives - Adobe AIR Multiple Flaws Let Remote Users Execute Arbitrary Code, Conduct Cross-Site Scripting Attacks, ar

Adobe Flash Player and AIR (CVE-2010-2185) Buffer Overflow Vulnerability

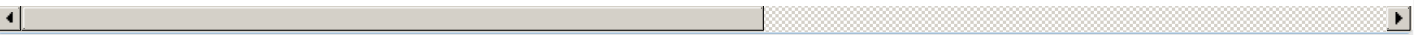
About the security content of Mac OS X v10.6.5 and Security Update 2010-007

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)