



# CVE-2010-2215

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

## Summary

|                 |                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2010-2215                                                                                                                                                                                                                                    |
| State           | PUBLISHED                                                                                                                                                                                                                                        |
| Assigner        | adobe                                                                                                                                                                                                                                            |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                                                                                                                                                     |
| Published       | 2010-08-11 18:47:50 UTC                                                                                                                                                                                                                          |
| Updated         | 2026-04-29 01:13:23 UTC                                                                                                                                                                                                                          |
| Description     | Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to trick a user into downloading and installing a malicious file, which can be used to execute arbitrary code on the victim's system. |

## Risk And Classification

**Primary CVSS:** v2.0 4.3 from nvd@nist.gov

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

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product   | Version | Update | Edition | Language |
|-------------|--------|-----------|---------|--------|---------|----------|
| Application | Adobe  | Adobe Air | All     | All    | All     | All      |

|             |                       |                              |              |     |     |     |
|-------------|-----------------------|------------------------------|--------------|-----|-----|-----|
| Application | <a href="#">Adobe</a> | <a href="#">Adobe Air</a>    | 1.0          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Adobe Air</a>    | 1.0.1        | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Adobe Air</a>    | 1.5          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Adobe Air</a>    | 1.5.1        | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Adobe Air</a>    | 1.5.3        | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Adobe Air</a>    | 1.5.3.9120   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | All          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.0.584   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.12.10   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.12.36   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.15.3    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.22.87   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.32.18   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.42.34   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.0.45.2    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.1.52.14.1 | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 10.1.52.15   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 7.0          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 7.0.1        | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 7.0.25       | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 7.0.63       | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 7.1.1        | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 7.2          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0.22.0     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0.33.0     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0.34.0     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0.35.0     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0.39.0     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 8.0.42.0     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 9.0          | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 9.0.112.0    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 9.0.114.0    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 9.0.115.0    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 9.0.124.0    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 9.0.125.0    | All | All | All |

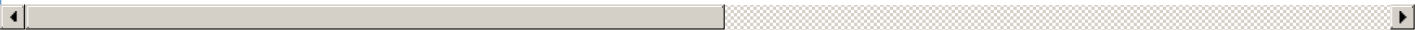
|             |                       |                                        |            |     |     |     |
|-------------|-----------------------|----------------------------------------|------------|-----|-----|-----|
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.151.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.152.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.159.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.16     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.18d60  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.20     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.20.0   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.246.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.260.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.28     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.28.0   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.31     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.31.0   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.45.0   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.47.0   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.0.48.0   | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | 9.125.0    | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a>           | All        | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 10.0.12.36 | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 10.0.15.3  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 9.0.115.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 9.0.124.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 9.0.151.0  | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 9.0.31     | All | All | All |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player For Linux</a> | 9.0.48.0   | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

References

| Reference                                                                                                     |
|---------------------------------------------------------------------------------------------------------------|
| Adobe - Security Bulletins: APSB10-16 Security update available for Adobe Flash Player                        |
| About the security content of Mac OS X v10.6.5 and Security Update 2010-007                                   |
| APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007                                           |
| '[security bulletin] HPSBMA02592 SSRT100300 rev.1 - HP Systems Insight Manager (SIM) for HP-UX, Linux' - MARC |

|                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------|
| Gentoo Linux Documentation -- Adobe Flash Player: Multiple vulnerabilities                                                            |
| Adobe Flash Player and AIR (CVE-2010-2215) Unspecified Clickjacking Vulnerability                                                     |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH                                                                      |
| Repository / Oval Repository                                                                                                          |
| Gentoo update for adobe-flash - Advisories - Community                                                                                |
| Repository / Oval Repository                                                                                                          |
| SecurityTracker.com Archives - HP Systems Insight Manager Flaws Let Remote Users Modify Data, Deny Service, or Execute Arbitrary Code |
| 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.                                                                  |