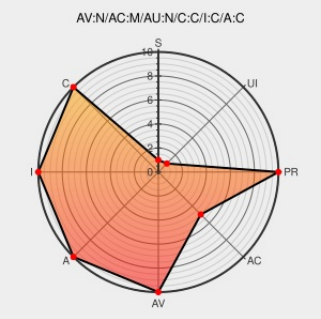
# CVE-2012-2035

Published on: 06/08/2012 12:00:00 AM UTC

Last Modified on: 09/08/2021 05:19:00 PM UTC

## CVE-2012-2035

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Air from Adobe contain the following vulnerability:

Stack-based buffer overflow in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code via unspecified vectors.

CVE-2012-2035 has been assigned by psirt@adobe.com to track the vulnerability

### CVSS2 Score: 9.3 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Adobe - Security Bulletins: APSB12-14 - Security updates available for Adobe Flash Player | Vendor Advisory, www.adobe.com, text/xml | CONFIRM www.adobe.com/support/security/bulletins/apsb12-14.html |
| Red Hat Customer Portal | Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived | REDHAT RHSA-2012:0722 |
| [security-announce] SUSE-SU-2012:0724-1: critical: Security update for f | Mailing List, Third Party Advisory, lists.opensuse.org, text/html | SUSE SUSE-SU-2012:0724 |
| [security-announce] openSUSE-SU-2012:0723-1: critical: | Mailing List | SUSE openSUSE-SU-2012:0723 |

flash-player: Upd

Third Party Advisory
lists.opensuse.org
text/html



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Adobe | Air | All | All | All | All |
| Application | Adobe | Flash Player | All | All | All | All |
| Application | Adobe | Flash Player | All | All | All | All |
| Application | Adobe | Flash Player | All | All | All | All |
| Operating System | Apple | Macos | - | All | All | All |
| Operating System | Apple | Mac Os | - | All | All | All |
| Operating System | Apple | Mac Os | - | All | All | All |
| Operating System | Google | Android | - | All | All | All |
| Operating System | Google | Android | All | All | All | All |
| Operating System | Google | Android | All | All | All | All |
| Operating System | Google | Android | - | All | All | All |
| Operating System | Google | Android | All | All | All | All |
| Operating System | Google | Android | All | All | All | All |
| Operating System | Linux | Linux Kernel | - | All | All | All |
| Operating System | Linux | Linux Kernel | - | All | All | All |
| Operating System | Microsoft | Windows | - | All | All | All |
| Operating System | Microsoft | Windows | - | All | All | All |
| Operating System | Opensuse | Opensuse | 11.4 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Opensuse | Opensuse | 12.1 | All | All | All |
| Operating System | Opensuse | Opensuse | 11.4 | All | All | All |
| Operating System | Opensuse | Opensuse | 12.1 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 6.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 6.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 6.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 6.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 10 | sp4 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp2 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 10 | sp4 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp1 | All | All |
| Operating System | Suse | Linux Enterprise Desktop | 11 | sp2 | All | All |

- cpe:2.3:a:adobe:air:*:*:*:*:*:*:*:*:
- cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:
- cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:
- cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:macos:-:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:-:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:
- cpe:2.3:o:google:android:*:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:
- cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux_eus:6.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:10:sp4:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:10:sp4:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→