



# CVE-2015-8648

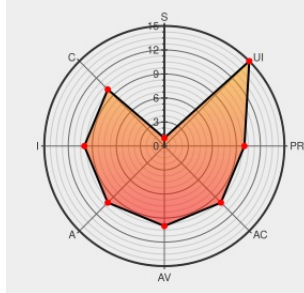
Published on: 12/28/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

## CVE-2015-8648

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Air](#) from [Adobe](#) contain the following vulnerability:

Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8649, and CVE-2015-8650.

CVE-2015-8648 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **9.3 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                         | Tags                          | Link                      |
|-------------------------------------|-------------------------------|---------------------------|
| Document Display LPE Support Center | <a href="#">CVE-2015-8648</a> | <a href="#">CONFIRMED</a> |

|                                                                                                    |                                                                                                                                                |                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Document Display   HPE Support Center                                                              | <a href="https://h20566.www2.hpe.com/text/html">h20566.www2.hpe.com<br/>text/html</a>                                                          |  CONFIRM<br><a href="https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05356388">h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05356388</a>   |
| Document Display   HPE Support Center                                                              | <a href="https://h20566.www2.hpe.com/text/html">h20566.www2.hpe.com<br/>text/html</a>                                                          |  CONFIRM<br><a href="https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722">h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722</a> |
| Adobe Flash Player Multiple Flaws Lets Remote Users Execute Arbitrary Code - SecurityTracker       | <a href="https://www.securitytracker.com/text/html">www.securitytracker.com<br/>text/html</a>                                                  |  SECTrack 1034544                                                                                                                                                                                   |
| [security-announce] SUSE-SU-2015:2401-1: important: Security update for                            | <a href="https://lists.opensuse.org/text/html">lists.opensuse.org<br/>text/html</a>                                                            |  SUSE SUSE-SU-2015:2401                                                                                                                                                                             |
| ZDI-15-652   Zero Day Initiative                                                                   | <a href="https://www.zerodayinitiative.com/text/html">www.zerodayinitiative.com<br/>text/html</a>                                              |  MISC <a href="https://www.zerodayinitiative.com/advisories/ZDI-15-652">www.zerodayinitiative.com/advisories/ZDI-15-652</a>                                                                         |
| [security-announce] openSUSE-SU-2015:2400-1: important: Security update                            | <a href="https://lists.opensuse.org/text/html">lists.opensuse.org<br/>text/html</a>                                                            |  SUSE openSUSE-SU-2015:2400                                                                                                                                                                         |
| Document Display   HPE Support Center                                                              | <a href="https://h20566.www2.hpe.com/text/html">h20566.www2.hpe.com<br/>text/html</a>                                                          |  CONFIRM<br><a href="https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680">h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680</a> |
| Red Hat Customer Portal                                                                            | <a href="https://web.archive.org/text/html">web.archive.org<br/>text/html</a><br><span>Inactive Link</span> <span>Not Archived</span>          |  REDHAT RHSA-2015:2697                                                                                                                                                                              |
| Adobe Security Bulletin                                                                            | <a href="#">Patch</a><br><a href="#">Vendor Advisory</a><br><a href="https://helpx.adobe.com">helpx.adobe.com</a><br><a href="#">text/html</a> |  CONFIRM <a href="https://helpx.adobe.com/security/products/flash-player/apsb16-01.html">helpx.adobe.com/security/products/flash-player/apsb16-01.html</a>                                          |
| Adobe Flash Player: Multiple vulnerabilities (GLSA 201601-03) — Gentoo Security                    | <a href="https://security.gentoo.org/text/html">security.gentoo.org<br/>text/html</a>                                                          |  GENTOO GLSA-201601-03                                                                                                                                                                            |
| Adobe Flash Player and AIR APSB16-01 Multiple Use After Free Remote Code Execution Vulnerabilities | <a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                                                                              |  BID 79701                                                                                                                                                                                        |
| [security-announce] openSUSE-SU-2015:2403-1: important: Security update                            | <a href="https://lists.opensuse.org/text/html">lists.opensuse.org<br/>text/html</a>                                                            |  SUSE openSUSE-SU-2015:2403                                                                                                                                                                       |
| [security-announce] SUSE-SU-2015:2402-1: important: Security update for                            | <a href="https://lists.opensuse.org/text/html">lists.opensuse.org<br/>text/html</a>                                                            |  SUSE SUSE-SU-2015:2402                                                                                                                                                                           |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type        | Vendor                | Product                          | Version | Update | Edition | Language |
|-------------|-----------------------|----------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Adobe</a> | <a href="#">Air</a>              | All     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Air Sdk</a>          | All     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Air Sdk Compiler</a> | All     | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Air Sdk Compiler</a> | All     | All    | All     | All      |

|                                                |           |              |            |     |     |     |
|------------------------------------------------|-----------|--------------|------------|-----|-----|-----|
| Application                                    | Adobe     | Flash Player | 19.0.0.185 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.207 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.226 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.245 | All | All | All |
| Application                                    | Adobe     | Flash Player | 20.0.0.228 | All | All | All |
| Application                                    | Adobe     | Flash Player | 20.0.0.235 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.185 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.207 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.226 | All | All | All |
| Application                                    | Adobe     | Flash Player | 19.0.0.245 | All | All | All |
| Application                                    | Adobe     | Flash Player | 20.0.0.228 | All | All | All |
| Application                                    | Adobe     | Flash Player | 20.0.0.235 | All | All | All |
| Application                                    | Adobe     | Flash Player | All        | All | All | All |
| Application                                    | Adobe     | Flash Player | All        | All | All | All |
| Operating System                               | Apple     | Iphone Os    | All        | All | All | All |
| Operating System                               | Apple     | Iphone Os    | All        | All | All | All |
| Operating System                               | Apple     | Mac Os X     | All        | All | All | All |
| Operating System                               | Apple     | Mac Os X     | All        | 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 | All |
| Operating System                               | Linux     | Linux Kernel | All        | All | All | All |
| Operating System                               | Microsoft | Windows      | All        | All | All | All |
| Operating System                               | Microsoft | Windows      | All        | All | All | All |
| cpe:2.3:a:adobe:air:*****:                     |           |              |            |     |     |     |
| cpe:2.3:a:adobe:air_sdk:*****:                 |           |              |            |     |     |     |
| cpe:2.3:a:adobe:air_sdk_&_compiler:*****:      |           |              |            |     |     |     |
| cpe:2.3:a:adobe:air_sdk_&_compiler:*****:      |           |              |            |     |     |     |
| cpe:2.3:a:adobe:flash_player:19.0.0.185:*****: |           |              |            |     |     |     |

|                                                |
|------------------------------------------------|
| cpe:2.3:a:adobe:flash_player:19.0.0.185:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.207:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.226:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.245:*****: |
| cpe:2.3:a:adobe:flash_player:20.0.0.228:*****: |
| cpe:2.3:a:adobe:flash_player:20.0.0.235:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.185:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.207:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.226:*****: |
| cpe:2.3:a:adobe:flash_player:19.0.0.245:*****: |
| cpe:2.3:a:adobe:flash_player:20.0.0.228:*****: |
| cpe:2.3:a:adobe:flash_player:20.0.0.235:*****: |
| cpe:2.3:a:adobe:flash_player:*****:            |
| cpe:2.3:a:adobe:flash_player:*****:            |
| cpe:2.3:o:apple:iphone_os:*****:               |
| cpe:2.3:o:apple:iphone_os:*****:               |
| cpe:2.3:o:apple:mac_os_x:*****:                |
| cpe:2.3:o:apple:mac_os_x:*****:                |
| 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:*****:             |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)