



# CVE-2016-4276

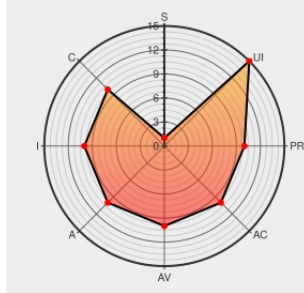
Published on: 09/14/2016 12:00:00 AM UTC

Last Modified on: 11/14/2022 07:34:00 PM UTC

## CVE-2016-4276

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.

CVE-2016-4276 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                                  |
|-------------------------|-------------------------------|---------------------------------------|
| Red Hat Customer Portal | <a href="#">CVE-2016-4276</a> | <a href="#">REDHAT-RHSA-2016-1865</a> |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                 |                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Red Hat Customer Portal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">web.archive.org</a><br><a href="#">text/html</a><br>Inactive Link Not Archived      |  <a href="#">RHSA-2016-1869</a>                                                                             |
| Adobe Flash Player Bugs Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code - SecurityTracker                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <a href="#">www.securitytracker.com</a><br><a href="#">text/html</a>                            |  <a href="#">SECTrack 1036791</a>                                                                         |
| Adobe Flash Player APSB16-29 Multiple Unspecified Memory Corruption Vulnerabilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                               |  <a href="#">BID 92930</a>                                                                                |
| Adobe Flash Player: Multiple vulnerabilities (GLSA 201610-10) — Gentoo security                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">security.gentoo.org</a><br><a href="#">text/html</a>                                |  <a href="#">GENTOO GLSA-201610-10</a>                                                                    |
| Adobe Security Bulletin                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <a href="#">Vendor Advisory</a><br><a href="#">helpx.adobe.com</a><br><a href="#">text/html</a> |  <a href="#">CONFIRM</a><br><a href="#">helpx.adobe.com/security/products/flash-player/apsb16-29.html</a> |
| <p>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 <a href="mailto:comment@cve.report">comment@cve.report</a>.</p> |                                                                                                 |                                                                                                                                                                                              |

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="#">Flash Player</a>                 | All     | 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>                 | All     | 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>                 | All     | 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 Desktop Runtime</a> | All     | All    | All     | All      |
| Operating System | <a href="#">Apple</a>  | <a href="#">Mac Os X</a>                     | All     | All    | All     | All      |
| Operating System | <a href="#">Apple</a>  | <a href="#">Mac Os X</a>                     | -       | All    | All     | All      |
| Operating System | <a href="#">Apple</a>  | <a href="#">Mac Os X</a>                     | All     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Chrome Os</a>                    | All     | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Chrome Os</a>                    | -       | All    | All     | All      |
| Operating System | <a href="#">Google</a> | <a href="#">Chrome Os</a>                    | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                 | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                 | -       | 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 |
| Operating System                                         | Microsoft | Windows      | All | All | All | All |
| Operating System                                         | Microsoft | Windows 10   | All | All | All | All |
| Operating System                                         | Microsoft | Windows 10   | -   | All | All | All |
| Operating System                                         | Microsoft | Windows 10   | All | All | All | All |
| Operating System                                         | Microsoft | Windows 8.1  | All | All | All | All |
| Operating System                                         | Microsoft | Windows 8.1  | -   | All | All | All |
| Operating System                                         | Microsoft | Windows 8.1  | All | All | All | All |
| cpe:2.3:a:adobe:flash_player:*****:                      |           |              |     |     |     |     |
| cpe:2.3:a:adobe:flash_player:*****:esr:***:              |           |              |     |     |     |     |
| cpe:2.3:a:adobe:flash_player:*****:                      |           |              |     |     |     |     |
| cpe:2.3:a:adobe:flash_player:*****:chrome:**:            |           |              |     |     |     |     |
| cpe:2.3:a:adobe:flash_player:*****:edge:**:              |           |              |     |     |     |     |
| cpe:2.3:a:adobe:flash_player:*****:internet_explorer:**: |           |              |     |     |     |     |
| cpe:2.3:a:adobe:flash_player_desktop_runtime:*****:      |           |              |     |     |     |     |
| cpe:2.3:o:apple:mac_os_x:*****:                          |           |              |     |     |     |     |
| cpe:2.3:o:apple:mac_os_x:-:*****:                        |           |              |     |     |     |     |
| cpe:2.3:o:apple:mac_os_x:*****:                          |           |              |     |     |     |     |
| cpe:2.3:o:google:chrome_os:*****:                        |           |              |     |     |     |     |
| cpe:2.3:o:google:chrome_os:-:*****:                      |           |              |     |     |     |     |
| cpe:2.3:o:google:chrome_os:*****:                        |           |              |     |     |     |     |
| cpe:2.3:o:linux:linux_kernel:*****:                      |           |              |     |     |     |     |
| 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:microsoft:windows:*.*.*.*.*.*.*.*.*       |
| cpe:2.3:o:microsoft:windows_10:*.*.*.*.*.*.*.*.*    |
| cpe:2.3:o:microsoft:windows_10:-.*.*.*.*.*.*.*.*.*  |
| cpe:2.3:o:microsoft:windows_10:*.*.*.*.*.*.*.*.*    |
| cpe:2.3:o:microsoft:windows_8.1:*.*.*.*.*.*.*.*.*   |
| cpe:2.3:o:microsoft:windows_8.1:-.*.*.*.*.*.*.*.*.* |
| cpe:2.3:o:microsoft:windows_8.1:*.*.*.*.*.*.*.*.*   |

```
cpe:2.3:o:microsoft:windows:*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:microsoft:windows 10:::*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:microsoft:windows 10:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows_10:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows 8.1:-:*:*:*:*:*:
```

```
cpe:2.3:o:microsoft:windows 8.1:*.~*~*~*~*~*~*~*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

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](https://status.cve.report)