



# CVE-2015-3041

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

## Summary

|                        |                                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2015-3041                                                                                                        |
| <b>State</b>           | PUBLIC                                                                                                               |
| <b>Assigner</b>        | psirt@adobe.com                                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                         |
| <b>Published</b>       | 2015-04-14 22:59:00 UTC                                                                                              |
| <b>Updated</b>         | 2018-10-30 16:27:00 UTC                                                                                              |
| <b>Description</b>     | Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202 |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                | Product                      | Version    | Update | Edition | Language |
|-------------|-----------------------|------------------------------|------------|--------|---------|----------|
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 14.0.0.125 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 14.0.0.145 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 14.0.0.176 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 14.0.0.179 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 15.0.0.152 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 15.0.0.167 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 15.0.0.189 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 15.0.0.223 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 15.0.0.239 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 15.0.0.246 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 16.0.0.235 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 16.0.0.257 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 16.0.0.287 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 16.0.0.296 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 17.0.0.134 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 14.0.0.125 | All    | All     | All      |
| Application | <a href="#">Adobe</a> | <a href="#">Flash Player</a> | 14.0.0.145 | All    | All     | All      |

|                  |           |                                           |            |     |     |     |
|------------------|-----------|-------------------------------------------|------------|-----|-----|-----|
|                  |           |                                           |            |     |     |     |
| Application      | Adobe     | Flash Player                              | 14.0.0.176 | All | All | All |
| Application      | Adobe     | Flash Player                              | 14.0.0.179 | All | All | All |
| Application      | Adobe     | Flash Player                              | 15.0.0.152 | All | All | All |
| Application      | Adobe     | Flash Player                              | 15.0.0.167 | All | All | All |
| Application      | Adobe     | Flash Player                              | 15.0.0.189 | All | All | All |
| Application      | Adobe     | Flash Player                              | 15.0.0.223 | All | All | All |
| Application      | Adobe     | Flash Player                              | 15.0.0.239 | All | All | All |
| Application      | Adobe     | Flash Player                              | 15.0.0.246 | All | All | All |
| Application      | Adobe     | Flash Player                              | 16.0.0.235 | All | All | All |
| Application      | Adobe     | Flash Player                              | 16.0.0.257 | All | All | All |
| Application      | Adobe     | Flash Player                              | 16.0.0.287 | All | All | All |
| Application      | Adobe     | Flash Player                              | 16.0.0.296 | All | All | All |
| Application      | Adobe     | Flash Player                              | 17.0.0.134 | All | All | All |
| Application      | Adobe     | Flash Player                              | All        | All | All | All |
| Application      | Adobe     | Flash Player                              | All        | All | All | All |
| Operating System | Apple     | Mac Os X                                  | -          | All | All | All |
| Operating System | Apple     | Mac Os X                                  | -          | 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                                  | 13.1       | All | All | All |
| Operating System | Opensuse  | Opensuse                                  | 13.2       | All | All | All |
| Operating System | Opensuse  | Opensuse                                  | 13.1       | All | All | All |
| Operating System | Opensuse  | Opensuse                                  | 13.2       | All | All | All |
| Operating System | Redhat    | Enterprise Linux Desktop Supplementary    | 5.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Desktop Supplementary    | 6.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Desktop Supplementary    | 5.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Desktop Supplementary    | 6.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Server Supplementary     | 5.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Server Supplementary     | 6.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Server Supplementary     | 5.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Server Supplementary     | 6.0        | All | All | All |
| Operating System | Redhat    | Enterprise Linux Server Supplementary Eus | 6.6.z      | All | All | All |
| Operating System | Redhat    | Enterprise Linux Server Supplementary Eus | 6.6.z      | All | All | All |

|                  |                        |                                                            |      |     |     |     |
|------------------|------------------------|------------------------------------------------------------|------|-----|-----|-----|
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation Supplementary</a> | 6.0  | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation Supplementary</a> | 6.0  | All | All | All |
| Operating System | <a href="#">Suse</a>   | <a href="#">Suse Linux Enterprise Desktop</a>              | 11.0 | sp3 | All | All |
| Operating System | <a href="#">Suse</a>   | <a href="#">Suse Linux Enterprise Desktop</a>              | 12.0 | All | All | All |
| Operating System | <a href="#">Suse</a>   | <a href="#">Suse Linux Enterprise Desktop</a>              | 11.0 | sp3 | All | All |
| Operating System | <a href="#">Suse</a>   | <a href="#">Suse Linux Enterprise Desktop</a>              | 12.0 | All | All | All |
| Operating System | <a href="#">Suse</a>   | <a href="#">Suse Linux Workstation Extension</a>           | 12.0 | All | All | All |
| Operating System | <a href="#">Suse</a>   | <a href="#">Suse Linux Workstation Extension</a>           | 12.0 | All | All | All |

| References                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Reference</b>                                                                                                                         |
| Red Hat Customer Portal                                                                                                                  |
| Adobe Flash Player Multiple Unspecified Memory Corruption Vulnerabilities                                                                |
| [security-announce] openSUSE-SU-2015:0725-1: important: Security update                                                                  |
| [security-announce] openSUSE-SU-2015:0718-1: important: Security update                                                                  |
| Adobe Flash Player: Multiple vulnerabilities (GLSA 201504-07) — Gentoo security                                                          |
| [security-announce] SUSE-SU-2015:0723-1: important: Security update for                                                                  |
| Adobe Security Bulletin                                                                                                                  |
| [security-announce] SUSE-SU-2015:0722-1: important: Security update for                                                                  |
| Adobe Flash Player Multiple Bugs Let Remote Users Bypass ASLR, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - Se |
| CVE Program record                                                                                                                       |
| NVD vulnerability detail                                                                                                                 |
| <div><div></div><div></div></div>                                                                                                        |

|                                                                      |
|----------------------------------------------------------------------|
| No vendor comments have been submitted for this CVE.                 |
| There are currently no legacy QID mappings associated with this CVE. |