



CVE-2016-0987

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2016-0987 |
| State | PUBLIC |
| Assigner | psirt@adobe.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-03-12 15:59:00 UTC |
| Updated | 2022-12-14 19:02:00 UTC |
| Description | Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows a |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------------------|------------|--------|---------|----------|
| Application | Adobe | Air | All | All | All | All |
| Application | Adobe | Air | All | All | All | All |
| Application | Adobe | Air Desktop Runtime | All | All | All | All |
| Application | Adobe | Air Sdk | All | All | All | All |
| Application | Adobe | Air Sdk Compiler | All | All | All | All |
| Application | Adobe | Air Sdk Compiler | 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 | 20.0.0.286 | 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 | 20.0.0.286 | 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 |
| Application | Adobe | Flash Player | All | All | All | All |
| Application | Adobe | Flash Player Desktop Runtime | All | All | All | All |
| Application | Adobe | Flash Player Esr | All | All | All | All |
| Operating System | Apple | Iphone Os | All | All | All | All |
| Operating System | Apple | Iphone Os | - | 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 |
| 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 |
| Operating System | Google | Android | All | All | All | All |
| Operating System | Google | Chrome Os | All | All | All | All |
| Operating System | Google | Chrome Os | - | All | All | All |
| Operating System | Google | Chrome Os | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | - | 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 |
| Operating System | Samsung | X14j Firmware | t-ms14jakucb-1102.5 | All | All | All |

References

| Reference | Source | Link |
|--|----------|--|
| Adobe Flash Player: Multiple vulnerabilities (GLSA 201603-07) — Gentoo Security | GENTOO | security.gentoo.org |
| Adobe Security Bulletin | CONFIRM | helpx.adobe.com |
| [security-announce] SUSE-SU-2016:0715-1: important: Security update for | SUSE | lists.opensuse.org |
| [security-announce] openSUSE-SU-2016:0734-1: important: Security update | SUSE | lists.opensuse.org |
| [security-announce] openSUSE-SU-2016:0719-1: important: Security update | SUSE | lists.opensuse.org |
| Adobe Flash Player Multiple Flaws Lets Remote Users Execute Arbitrary Code - SecurityTracker | SECTRACK | www.securitytracker.com |
| Adobe Flash Player and AIR APSB16-08 Multiple Use After Free Remote Code Execution Vulnerabilities | BID | www.securityfocus.com |
| [security-announce] SUSE-SU-2016:0716-1: important: Security update for | SUSE | lists.opensuse.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

CVE.report and Source URL Uptime Status status.cve.report