



CVE-2007-0045

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2007-0045 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2007-01-03 21:28:00 UTC |
| Updated | 2018-10-16 16:30:00 UTC |
| Description | Multiple cross-site scripting (XSS) vulnerabilities in Adobe Acrobat Reader Plugin before 8.0.0, and possibly the plugin distr |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|-----------------------|-------------------------|---------|--------|--------------|----------|
| Application | Adobe | Acrobat | 7.0 | All | professional | All |
| Application | Adobe | Acrobat | 7.0 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.1 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.1 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.2 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.2 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.3 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.3 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.4 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.4 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.5 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.5 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.6 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.6 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.7 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.7 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.8 | All | professional | All |

| | | | | | | |
|-------------|-------|----------------|-------|-----|--------------|-----|
| Application | Adobe | Acrobat | 7.0.8 | All | standard | All |
| Application | Adobe | Acrobat | 7.0 | All | professional | All |
| Application | Adobe | Acrobat | 7.0 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.1 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.1 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.2 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.2 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.3 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.3 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.4 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.4 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.5 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.5 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.6 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.6 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.7 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.7 | All | standard | All |
| Application | Adobe | Acrobat | 7.0.8 | All | professional | All |
| Application | Adobe | Acrobat | 7.0.8 | All | standard | All |
| Application | Adobe | Acrobat | All | All | elements | All |
| Application | Adobe | Acrobat 3d | All | All | All | All |
| Application | Adobe | Acrobat 3d | All | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.1 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.2 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.3 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.4 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.5 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.1 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.2 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.3 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.4 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.5 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.6 | All | All | All |

| | | | | | | |
|-------------|-----------------------|--------------------------------|-------|-----|-----|-----|
| Application | Adobe | Acrobat Reader | 7.0.7 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.8 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.1 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.2 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.3 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.4 | All | All | All |
| Application | Adobe | Acrobat Reader | 6.0.5 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.1 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.2 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.3 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.4 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.5 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.6 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.7 | All | All | All |
| Application | Adobe | Acrobat Reader | 7.0.8 | All | All | All |
| Application | Adobe | Acrobat Reader | All | All | All | All |

References

Reference

The Slackware Linux Project: Slackware Security Advisories

rhn.redhat.com | Red Hat Support

Google Chrome Cross-Site Scripting and Information Disclosure - Advisories - Community

SecurityFocus

Wisec - The Wise SECURITY

US-CERT Vulnerability Note VU#815960

Universal PDF XSS After Party | GNUCITIZEN

SecurityFocus

Adobe - Security Advisories : Update available for vulnerabilities in versions 7.0.8 and earlier of Adobe Reader and Acrobat

MFSA 2007-02: Improvements to help protect against Cross-Site Scripting attacks

Adobe Acrobat Reader: Multiple vulnerabilities — Gentoo Linux Documentation

rhn.redhat.com | Red Hat Support

102847

Slackware update for seamonkey - Advisories - Secunia

Google Chrome Releases: Stable, Beta update: Yahoo! Mail and Security Fixes

| |
|---|
| Red Hat update for acroread - Advisories - Secunia |
| Sun Solaris Adobe Acrobat Multiple Vulnerabilities - Advisories - Secunia |
| US-CERT Technical Cyber Security Alert TA09-286B -- Adobe Reader and Acrobat Vulnerabilities |
| SecurityTracker.com Archives - Adobe Acrobat and Adobe Reader Flaws Lets Remote Users Execute Arbitrary Code and Deny Service |
| SecurityReason - Adobe Acrobat Reader Plugin - Multiple Vulnerabilities |
| SecurityFocus |
| Adobe Reader Plugin Open Parameters Cross-Site Scripting Vulnerability |
| SUSE update for acroread - Advisories - Secunia |
| Hacking with Browser Plugins at Disenchant's Blog |
| SecurityFocus |
| HPSBUX02153 SSRT061181 rev.7 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS) |
| Adobe - Security Bulletin APSB09-15 Security Updates Available for Adobe Reader and Acrobat |
| SecurityFocus |
| Repository / Oval Repository |
| Red Hat update for acroread - Advisories - Secunia |
| Gentoo update for acroread - Advisories - Secunia |
| About Secunia Research Flexera |
| DANGER, DANGER, DANGER GNUCITIZEN |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| IBM X-Force Exchange |
| Adobe - Cross-site scripting vulnerability in versions 7.0.8 and earlier of Adobe Reader and Acrobat |
| SecurityTracker.com Archives - Adobe Acrobat Reader Plugin Bugs Let Remote Users Deny Service, Conduct Cross-Site Scripting Attacks, and |
| Adobe - Server-side workarounds to prevent potential cross-site scripting vulnerability in versions 7.0.8 and earlier of Adobe Reader and Acrobat |
| SecurityFocus |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| events.ccc.de/congress/2006/Fahrplan/attachments/1158-Subverting_Ajax.pdf |
| Repository / Oval Repository |
| SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: Acrobat Reader 7.0.9 (SUSE-SA:2007:011) |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| CVE Program record |
| NVD vulnerability detail |

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](#) 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](#)