



CVE-2008-4401

Published on: 10/17/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:10 PM UTC

CVE-2008-4401

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

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

ActionScript in Adobe Flash Player 9.0.124.0 and earlier does not require user interaction in conjunction with (1) the `FileReference.browse` operation in the `FileReference` upload API or (2) the `FileReference.download` operation in the `FileReference` download API, which allows remote attackers to create a browse dialog box, and possibly have unspecified other impact, via an SWF file.

CVE-2008-4401 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:025	lists.opensuse.org text/html	SUSE SUSE-SR:2008:025
Red Hat Customer Portal	www.redhat.com text/html	REDHAT RHSA-2008:0945
Gentoo update for netscape-flash - Secunia Advisories - Vulnerability Information - Secunia.com	web.archive.org text/html	SECUNIA 34226
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF adobe-flash-filereference-file-upload(45913)

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 32759
ASA-2009-020 (SUN 248586)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2009-020.htm
SecurityTracker.com Archives - Adobe Flash FileReference API Lets Remote Users Execute Arbitrary Code	securitytracker.com text/html	 SECTrack 1021061
Red Hat update for flash-plugin - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 32448
About Secunia Research Flexera	secunia.com Depreciated Link text/plain	 SECUNIA 33390
ASA-2008-440 (RHSA-2008-0980)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2008-440.htm
Support	www.redhat.com text/html	 REDHAT RHSA-2008:0980
Gentoo Linux Documentation -- Adobe Flash Player: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-200903-23
Red Hat update for flash-plugin - Secunia Advisories - Vulnerability Intelligence - Secunia.com	web.archive.org text/html	 SECUNIA 32702
Adobe - Developer Center : Understanding the security changes in Flash Player 10	www.adobe.com text/xml	 CONFIRM www.adobe.com/devnet/flashplayer/articles/fplayer10_security_changes.html
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2008-2838
About Secunia Research Flexera	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 32270
Adobe - Security Advisories : APSB08-18: Flash Player update available to address security vulnerabilities	Patch Vendor Advisory www.adobe.com text/xml	 CONFIRM www.adobe.com/support/security/bulletins/apsb08-18.html
No Description Provided	sunsolve.sun.com Inactive Link Not Archived	 SUNALERT 248586

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.

There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	7.0	All	All	All
Application	Adobe	Flash Player	7.0.1	All	All	All
Application	Adobe	Flash Player	7.0.25	All	All	All
Application	Adobe	Flash Player	7.0.63	All	All	All
Application	Adobe	Flash Player	7.0.69.0	All	All	All
Application	Adobe	Flash Player	7.0.70.0	All	All	All
Application	Adobe	Flash Player	7.0_r67	All	All	All
Application	Adobe	Flash Player	7.1	All	All	All
Application	Adobe	Flash Player	7.1.1	All	All	All
Application	Adobe	Flash Player	7.2	All	All	All
Application	Adobe	Flash Player	8.0	All	All	All
Application	Adobe	Flash Player	8.0.24.0	All	All	All
Application	Adobe	Flash Player	8.0.34.0	All	All	All
Application	Adobe	Flash Player	8.0.35.0	All	All	All
Application	Adobe	Flash Player	8.0.39.0	All	All	All
Application	Adobe	Flash Player	9.0	All	All	All
Application	Adobe	Flash Player	9.0.112.0	All	All	All
Application	Adobe	Flash Player	9.0.114.0	All	All	All
Application	Adobe	Flash Player	9.0.115.0	All	All	All
Application	Adobe	Flash Player	7.0	All	All	All
Application	Adobe	Flash Player	7.0.1	All	All	All
Application	Adobe	Flash Player	7.0.25	All	All	All
Application	Adobe	Flash Player	7.0.63	All	All	All
Application	Adobe	Flash Player	7.0.69.0	All	All	All
Application	Adobe	Flash Player	7.0.70.0	All	All	All
Application	Adobe	Flash Player	7.0_r67	All	All	All
Application	Adobe	Flash Player	7.1	All	All	All
Application	Adobe	Flash Player	7.1.1	All	All	All
Application	Adobe	Flash Player	7.2	All	All	All
Application	Adobe	Flash Player	8.0	All	All	All
Application	Adobe	Flash Player	8.0.24.0	All	All	All

Application	Adobe	Flash Player	8.0.34.0	All	All	All
Application	Adobe	Flash Player	8.0.35.0	All	All	All
Application	Adobe	Flash Player	8.0.39.0	All	All	All
Application	Adobe	Flash Player	9.0	All	All	All
Application	Adobe	Flash Player	9.0.112.0	All	All	All
Application	Adobe	Flash Player	9.0.114.0	All	All	All
Application	Adobe	Flash Player	9.0.115.0	All	All	All
Application	Adobe	Flash Player	All	All	All	All
cpe:2.3:a:adobe:flash_player:7.0:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.1:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.25:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.63:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.69.0:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.70.0:*****:*						
cpe:2.3:a:adobe:flash_player:7.0_r67:*****:*						
cpe:2.3:a:adobe:flash_player:7.1:*****:*						
cpe:2.3:a:adobe:flash_player:7.1.1:*****:*						
cpe:2.3:a:adobe:flash_player:7.2:*****:*						
cpe:2.3:a:adobe:flash_player:8.0:*****:*						
cpe:2.3:a:adobe:flash_player:8.0.24.0:*****:*						
cpe:2.3:a:adobe:flash_player:8.0.34.0:*****:*						
cpe:2.3:a:adobe:flash_player:8.0.35.0:*****:*						
cpe:2.3:a:adobe:flash_player:8.0.39.0:*****:*						
cpe:2.3:a:adobe:flash_player:9.0:*****:*						
cpe:2.3:a:adobe:flash_player:9.0.112.0:*****:*						
cpe:2.3:a:adobe:flash_player:9.0.114.0:*****:*						
cpe:2.3:a:adobe:flash_player:9.0.115.0:*****:*						
cpe:2.3:a:adobe:flash_player:7.0:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.1:*****:*						
cpe:2.3:a:adobe:flash_player:7.0.25:*****:*						

cpe:2.3:a:adobe:flash_player:7.0.63:*****:
cpe:2.3:a:adobe:flash_player:7.0.69.0:*****:
cpe:2.3:a:adobe:flash_player:7.0.70.0:*****:
cpe:2.3:a:adobe:flash_player:7.0_r67:*****:
cpe:2.3:a:adobe:flash_player:7.1:*****:
cpe:2.3:a:adobe:flash_player:7.1.1:*****:
cpe:2.3:a:adobe:flash_player:7.2:*****:
cpe:2.3:a:adobe:flash_player:8.0:*****:
cpe:2.3:a:adobe:flash_player:8.0.24.0:*****:
cpe:2.3:a:adobe:flash_player:8.0.34.0:*****:
cpe:2.3:a:adobe:flash_player:8.0.35.0:*****:
cpe:2.3:a:adobe:flash_player:8.0.39.0:*****:
cpe:2.3:a:adobe:flash_player:9.0:*****:
cpe:2.3:a:adobe:flash_player:9.0.112.0:*****:
cpe:2.3:a:adobe:flash_player:9.0.114.0:*****:
cpe:2.3:a:adobe:flash_player:9.0.115.0:*****:
cpe:2.3:a:adobe:flash_player:*****:

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