



CVE-2005-3525

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

CVE-2005-3525

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Stack-based buffer overflow in an ActiveX control for the installer for Adobe Macromedia Shockwave Player 10.1.0.11 and earlier allows remote attackers to execute arbitrary code via crafted large values for unspecified parameters.

CVE-2005-3525 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Macromedia - APSB06-02: Improper Memory Access Vulnerability in Adobe Shockwave Player

www.macromedia.com
[text/xml](#)

CONFIRM
www.macromedia.com/devnet/security/security_zone/apsb06-02.html

SecurityTracker.com Archives - Shockwave Player Buffer Overflow in ActiveX Installer Lets Remote Users Execute Arbitrary Code

securitytracker.com
[text/html](#)

SECTrack 1015673

Secunia - Advisories - Macromedia ShockWave Player ActiveX Installer Buffer Overflow

[Vendor Advisory](#)
web.archive.org
[text/html](#)

SECUNIA 19009

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
[text/html](#)

XF shockwave-activex-installer-bo(24914)

Macromedia Shockwave Player ActiveX Control Buffer Overflow Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

BID 16791

SecurityReason	securityreason.com text/html	SREASON 481
US-CERT Vulnerability Note VU#437212	US Government Resource www.kb.cert.org text/html	CERT-VN VU#437212
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060223 ZDI-06-002: Adobe Macromedia ShockWave Code Execution
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-0716
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 23461
ZDI-06-002 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-06-002.html

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	Shockwave Player	1.0	All	All	All
Application	Adobe	Shockwave Player	10.1.0.11	All	All	All
Application	Adobe	Shockwave Player	2.0	All	All	All
Application	Adobe	Shockwave Player	3.0	All	All	All
Application	Adobe	Shockwave Player	4.0	All	All	All
Application	Adobe	Shockwave Player	5.0	All	All	All
Application	Adobe	Shockwave Player	6.0	All	All	All
Application	Adobe	Shockwave Player	8.0	All	All	All
Application	Adobe	Shockwave Player	8.5.1	All	All	All
Application	Adobe	Shockwave Player	1.0	All	All	All
Application	Adobe	Shockwave Player	10.1.0.11	All	All	All
Application	Adobe	Shockwave Player	2.0	All	All	All
Application	Adobe	Shockwave Player	3.0	All	All	All
Application	Adobe	Shockwave Player	4.0	All	All	All
Application	Adobe	Shockwave Player	5.0	All	All	All
Application	Adobe	Shockwave Player	6.0	All	All	All
Application	Adobe	Shockwave Player	8.0	All	All	All

Application	Adobe	Shockwave Player	8.5.1	All	All	All
cpe:2.3:a:adobe:shockwave_player:1.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:10.1.0.11:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:2.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:3.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:4.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:5.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:6.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:8.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:8.5.1:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:1.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:10.1.0.11:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:2.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:3.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:4.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:5.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:6.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:8.0:*****:.*:						
cpe:2.3:a:adobe:shockwave_player:8.5.1:*****:.*:						

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](#)