

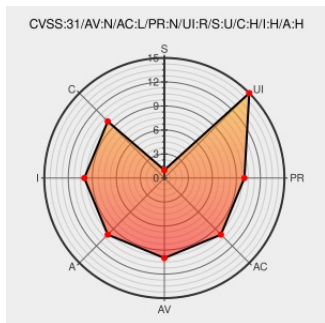


CVE-2010-1280

Published on: 05/13/2010 12:00:00 AM UTC

Last Modified on: 09/16/2022 06:19:00 PM UTC

CVE-2010-1280

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

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

Adobe Shockwave Player before 11.5.7.609 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted .dir (aka Director) file, related to (1) an erroneous dereference and (2) a certain Shock.dir file.

CVE-2010-1280 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

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
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20100512 [CAL-20100204-3]Adobe Shockwave Player Director File Parsing RCSL Pointer Overwrite
Zero Science Lab » Adobe Shockwave Player	Exploit	MISC www.zeroscience.mk/en/vulnerabilities/ZSL-

11.5.6.606 (DIR) Multiple Memory Vulnerabilities	www.zeroscience.mk text/html	2010-4937.php
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html Inactive Link Not Archived	 FULLDISC 20100511 [CAL-20100204-3]Adobe Shockwave Player Director File Parsing RCSL Pointer Overwrite
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Patch Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2010-1128
Adobe Shockwave Player Multiple Vulnerabilities - Advisories - Community	Vendor Advisory web.archive.org text/html	 SECUNIA 38751
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:7184
	Exploit www.zeroscience.mk text/x-c	 MISC www.zeroscience.mk/codes/shockwave_mem.txt
Adobe - Security Bulletins: APSB10-12 - Security update available for Shockwave Player	Patch Vendor Advisory www.adobe.com text/xml	 CONFIRM www.adobe.com/support/security/bulletins/apsb10-12.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	All	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	11.0.0.456	All	All	All
Application	Adobe	Shockwave Player	11.5.0.595	All	All	All
Application	Adobe	Shockwave Player	11.5.0.596	All	All	All
Application	Adobe	Shockwave Player	11.5.1.601	All	All	All
Application	Adobe	Shockwave Player	11.5.2.602	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	9	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	11.0.0.456	All	All	All
Application	Adobe	Shockwave Player	11.5.0.595	All	All	All
Application	Adobe	Shockwave Player	11.5.0.596	All	All	All
Application	Adobe	Shockwave Player	11.5.1.601	All	All	All
Application	Adobe	Shockwave Player	11.5.2.602	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	9	All	All	All
Application	Adobe	Shockwave Player	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Mac Os	All	All	All	All
Operating System	Apple	Mac Os	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
cpe:2.3:a:adobe:shockwave_player:*****:						
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:11.0.0.456:*****:						
cpe:2.3:a:adobe:shockwave_player:11.5.0.595:*****:						
cpe:2.3:a:adobe:shockwave_player:11.5.0.596:*****:						
cpe:2.3:a:adobe:shockwave_player:11.5.1.601:*****:						

cpe:2.3:a:adobe:shockwave_player:11.5.2.602:*****:
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:9:*****:
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:11.0.0.456:*****:
cpe:2.3:a:adobe:shockwave_player:11.5.0.595:*****:
cpe:2.3:a:adobe:shockwave_player:11.5.0.596:*****:
cpe:2.3:a:adobe:shockwave_player:11.5.1.601:*****:
cpe:2.3:a:adobe:shockwave_player:11.5.2.602:*****:
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:9:*****:
cpe:2.3:a:adobe:shockwave_player:*****:
cpe:2.3:o:apple:macos:*****:
cpe:2.3:o:apple:mac_os:*****:
cpe:2.3:o:apple:mac_os:*****:
cpe:2.3:o:microsoft:windows:*****:

cpe:2.3:o:microsoft:windows:

cpe:2.3:o:microsoft:windows:*****:

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](#)