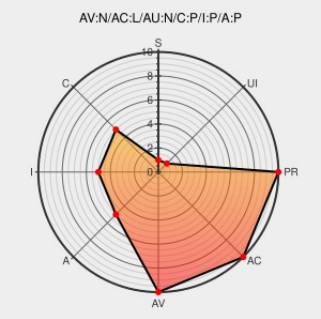
CVE-2010-2861

Published on: 08/11/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:08 PM UTC

CVE-2010-2861

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Coldfusion from Adobe contain the following vulnerability:

Multiple directory traversal vulnerabilities in the administrator console in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read arbitrary files via the locale parameter to (1) CFIDE/administrator/settings/mappings.cfm, (2) logging/settings.cfm, (3) datasources/index.cfm, (4) j2eepackaging/editarchive.cfm, and (5) enter.cfm in CFIDE/administrator/.

CVE-2010-2861 has been assigned by psirt@adobe.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ProCheckUp - Penetration Testing, PCI DSS Compliance, Application Testing	web.archive.org text/html Inactive Link Not Archived	MISC www.procheckup.com/vulnerability_manager/vulnerabilities/pr10-07
CXSecurity - IDS	securityreason.com text/html	SREASON 8137
ColdFusion directory traversal FAQ (CVE-2010-2861) | GNUCITIZEN	www.gnucitizen.org text/html	MISC www.gnucitizen.org/blog/coldfusion-directory-traversal-faq-cve-2010-2861/
Adobe - Security Bulletins: APSB10-18 Security update: Hotfix available for ColdFusion	Vendor Advisory www.adobe.com text/xml	CONFIRM www.adobe.com/support/security/bulletins/apsb10-18.html

CXSecurity - IDS securityreason.com text/html SREASON 8148

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	Coldfusion	8.0	All	All	All
Application	Adobe	Coldfusion	8.0.1	All	All	All
Application	Adobe	Coldfusion	9.0	All	All	All
Application	Adobe	Coldfusion	8.0	All	All	All
Application	Adobe	Coldfusion	8.0.1	All	All	All
Application	Adobe	Coldfusion	9.0	All	All	All
Application	Adobe	Coldfusion	All	All	All	All

cpe:2.3:a:adobe:coldfusion:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:8.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:8.0:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:8.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/coldfusion	List of CFML Vulnerabilities & Security Issues	2020-09-02 04:44:41

← 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 registred 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