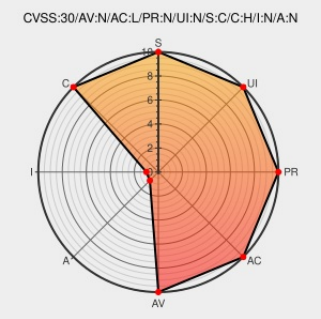
CVE-2016-4264

Published on: 09/01/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2016-4264

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



Certain versions of Coldfusion from Adobe contain the following vulnerability:

The Office Open XML (OOXML) feature in Adobe ColdFusion 10 before Update 21 and 11 before Update 10 allows remote attackers to read arbitrary files or send TCP requests to intranet servers via a crafted OOXML spreadsheet containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

CVE-2016-4264 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.6 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Adobe Security Bulletin	Vendor Advisory helpx.adobe.com	CONFIRM helpx.adobe.com/security/products/coldfusion/apsb16-

	text/html	30.html
	Exploit Third Party Advisory legalhackers.com text/plain	MISC legalhackers.com/advisories/Adobe-ColdFusion-11-XXE-Exploit-CVE-2016-4264.txt
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection - Multiple webapps Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 40346
Adobe ColdFusion XML Entity Parsing Bug Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036708
Adobe ColdFusion CVE-2016-4264 XML External Entity Information Disclosure Vulnerability	cve.report (archive) text/html	BID 92684
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20160907 CVE-2016-4264 Adobe ColdFusion <= 11 XXE Vulnerability

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	All	update21	All	All
Application	Adobe	Coldfusion	All	update10	All	All

cpe:2.3:a:adobe:coldfusion:*:update21:*:*:*:*:*:*:

cpe:2.3:a:adobe:coldfusion:*:update10:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→