



CVE-2017-3066

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3066
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-27 14:59:00 UTC
Updated	2026-04-22 12:14:13 UTC
Description	Adobe ColdFusion 2016 Update 3 and earlier, ColdFusion 11 update 11 and earlier, ColdFusion 10 Update 22 and earlier

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.936820000 probability, percentile 0.998500000 (date 2026-04-25)

CISA KEV: Listed on 2025-02-24; due 2025-03-17; ransomware use Unknown

Problem Types: CWE-502 | Code Injection | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

CISA Known Exploited Vulnerability

Vendor	Adobe
Product	ColdFusion
Name	Adobe ColdFusion Deserialization Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://helpx.adobe.com/security/products/coldfusion/apsb17-14.html ; https://nvd.nist.gov/vuln/detail/CVE-2017-3066

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Coldfusion	10.0	-	All	All
Application	Adobe	Coldfusion	10.0	update1	All	All
Application	Adobe	Coldfusion	10.0	update10	All	All
Application	Adobe	Coldfusion	10.0	update11	All	All

Application	Adobe	Coldfusion	10.0	update12	All	All
Application	Adobe	Coldfusion	10.0	update13	All	All
Application	Adobe	Coldfusion	10.0	update14	All	All
Application	Adobe	Coldfusion	10.0	update15	All	All
Application	Adobe	Coldfusion	10.0	update16	All	All
Application	Adobe	Coldfusion	10.0	update17	All	All
Application	Adobe	Coldfusion	10.0	update18	All	All
Application	Adobe	Coldfusion	10.0	update19	All	All
Application	Adobe	Coldfusion	10.0	update2	All	All
Application	Adobe	Coldfusion	10.0	update20	All	All
Application	Adobe	Coldfusion	10.0	update21	All	All
Application	Adobe	Coldfusion	10.0	update22	All	All
Application	Adobe	Coldfusion	10.0	update3	All	All
Application	Adobe	Coldfusion	10.0	update4	All	All
Application	Adobe	Coldfusion	10.0	update5	All	All
Application	Adobe	Coldfusion	10.0	update6	All	All
Application	Adobe	Coldfusion	10.0	update7	All	All
Application	Adobe	Coldfusion	10.0	update8	All	All
Application	Adobe	Coldfusion	10.0	update9	All	All
Application	Adobe	Coldfusion	11.0	-	All	All
Application	Adobe	Coldfusion	11.0	update1	All	All
Application	Adobe	Coldfusion	11.0	update10	All	All
Application	Adobe	Coldfusion	11.0	update11	All	All
Application	Adobe	Coldfusion	11.0	update2	All	All
Application	Adobe	Coldfusion	11.0	update3	All	All
Application	Adobe	Coldfusion	11.0	update4	All	All
Application	Adobe	Coldfusion	11.0	update5	All	All
Application	Adobe	Coldfusion	11.0	update6	All	All
Application	Adobe	Coldfusion	11.0	update7	All	All
Application	Adobe	Coldfusion	11.0	update8	All	All
Application	Adobe	Coldfusion	11.0	update9	All	All
Application	Adobe	Coldfusion	2016	-	All	All
Application	Adobe	Coldfusion	2016	update1	All	All
Application	Adobe	Coldfusion	2016	update2	All	All
Application	Adobe	Coldfusion	2016	update3	All	All

Vendor Declared Affected Products

Source	Vendor	Product
--------	--------	---------

CNA	Na	Adobe ColdFusion ColdFusion 2016 Update 3 And Earlier ColdFusion 11 Update 11 And Earlier ColdFusion 10 Update 2
-----	----	--

References

Reference

Adobe Security Bulletin

Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution - Windows remote Exploit

Adobe ColdFusion Java Deserialization Bug May Let Remote Users Execute Arbitrary Code and Input Validation Flaw Lets Remote Users Co

www.cisa.gov/known-exploited-vulnerabilities-catalog

Adobe Flex BlazeDS CVE-2017-3066 Remote Code Execution Vulnerability

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2025-02-24T00:00:00.000Z	CVE-2017-3066 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report