



Advisory NCSC-2026-0435

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Adobe ColdFusion

Publicatiedatum: 16-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe ColdFusion.

Duiding

De kwetsbaarheden in Adobe ColdFusion omvatten onder andere Server-Side Request Forgery (SSRF), Incorrect Authorization, Improper Input Validation, code-injectie, XML External Entity (XXE), Uncontrolled Resource Consumption en path traversal.

Aanvallers kunnen deze kwetsbaarheden misbruiken om zonder enige gebruikersinteractie privileges te escaleren, arbitrary code uit te voeren, bestanden te uploaden zonder restricties, interne resources te benaderen, gevoelige geheugeninformatie te onthullen, en denial-of-service te veroorzaken.

Sommige kwetsbaarheden zijn afhankelijk van externe factoren die de kans op succesvolle exploitatie beïnvloeden. De SSRF-kwetsbaarheden maken het mogelijk om netwerksegmentatie te omzeilen en toegang te krijgen tot interne systemen. De path traversal kwetsbaarheid in de Remote Development Services (RDS) functionaliteit stelt een aanvaller in staat om willekeurige bestanden te lezen zonder gebruikersinteractie, waarbij RDS standaard uitgeschakeld is in de Production Secure Profile. De kwetsbaarheden beïnvloeden de vertrouwelijkheid, integriteit en beschikbaarheid van ColdFusion-omgevingen.

Oplossingen

Adobe heeft updates uitgebracht om de kwetsbaarheden in ColdFusion te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.adobe.com/trust/security/products/coldfusion/apsb26-144.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-105897	8.6 HIGH
CVE-2026-105898	8.2 HIGH
CVE-2026-105899	10.0 CRITICAL
CVE-2026-105900	7.5 HIGH
CVE-2026-105901	8.8 HIGH
CVE-2026-105903	9.9 CRITICAL
CVE-2026-105994	7.7 HIGH
CVE-2026-106089	8.8 HIGH
CVE-2026-106090	8.8 HIGH
CVE-2026-106612	9.9 CRITICAL
CVE-2026-106613	8.8 HIGH
CVE-2026-106614	7.8 HIGH
CVE-2026-106615	8.8 HIGH
CVE-2026-106616	8.6 HIGH
CVE-2026-106617	8.8 HIGH
CVE-2026-106618	8.8 HIGH
CVE-2026-106619	9.0 CRITICAL
CVE-2026-106620	9.6 CRITICAL
CVE-2026-106621	9.1 CRITICAL
CVE-2026-106622	10.0 CRITICAL
CVE-2026-106623	7.5 HIGH
CVE-2026-106624	10.0 CRITICAL
CVE-2026-34633	7.7 HIGH
CVE-2026-34634	8.6 HIGH
CVE-2026-48378	5.3 MEDIUM
CVE-2026-71385	8.4 HIGH
CVE-2026-75748	7.6 HIGH
CVE-2026-75994	9.6 CRITICAL

CVE	CVSS Score
CVE-2026-75995	8.4 HIGH
CVE-2026-75996	7.5 HIGH
CVE-2026-76001	7.1 HIGH
CVE-2026-90530	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-611	Improper Restriction of XML External Entity Reference
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Adobe
ColdFusion
ColdFusion 2023
ColdFusion 2025

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:

NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.