Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0217

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 01-07-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Adobe heeft meerdere kwetsbaarheden verholpen in Adobe ColdFusion versies 25.9, 23.20 en eerdere versies.

Duiding

De kwetsbaarheden in Adobe ColdFusion betreffen onder andere onbeperkte upload van gevaarlijke bestandstypen, improper input validation, path traversal, reflected Cross-Site Scripting (XSS) en Server-Side Request Forgery (SSRF). Deze kwetsbaarheden maken het mogelijk voor een aanvaller om zonder enige gebruikersinteractie willekeurige code uit te voeren, bestanden te lezen of te schrijven, en beveiligingsmaatregelen te omzeilen. De path traversal kwetsbaarheden kunnen leiden tot toegang tot en wijziging van bestanden buiten de bedoelde directories. De XSS-kwetsbaarheid ontstaat door onvoldoende sanering van gebruikersinvoer in URL's, waardoor kwaadaardige scripts kunnen worden geïnjecteerd en uitgevoerd in de browser van een gebruiker. De SSRF-kwetsbaarheid stelt een aanvaller in staat om server-side verzoeken te manipuleren en ongeautoriseerde toegang tot bronnen te verkrijgen. Deze problemen zijn aanwezig in meerdere versies van ColdFusion, wat wijst op een breed impactgebied binnen de productlijn.

Oplossingen

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

Referenties

- https://helpx.adobe.com//security/products/coldfusion/apsb26-68.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-48276	10.0 CRITICAL
CVE-2026-48277	10.0 CRITICAL
CVE-2026-48281	10.0 CRITICAL
CVE-2026-48282	10.0 CRITICAL
CVE-2026-48283	10.0 CRITICAL

CVE-2026-48313	9.3 CRITICAL
CVE-2026-48315	9.3 CRITICAL
CVE-2026-48307	8.8 HIGH
CVE-2026-48285	8.6 HIGH
CVE-2026-48314	6.5 MEDIUM
CVE-2026-48316	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-434	Unrestricted Upload of File with Dangerous Type
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 of 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.