Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0362

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-09-2026

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.

Duiding

De kwetsbaarheden in Adobe ColdFusion omvatten onder andere een stored Cross-Site Scripting (XSS) waarbij een aanvaller met lage privileges kwaadaardige scripts kan injecteren in formulier velden die vervolgens uitgevoerd worden in de browser van een gebruiker. Daarnaast is er een kwetsbaarheid in de dynamische code-evaluatie die het mogelijk maakt voor een aanvaller met lage privileges om zonder gebruikersinteractie willekeurige code op afstand uit te voeren door onvoldoende neutralisatie van directives. Verder is er een SQL-injectie kwetsbaarheid die een aanvaller met hoge privileges in staat stelt om de SQL-querylogica te manipuleren en zo willekeurige code uit te voeren zonder gebruikersinteractie. Er zijn ook reflected XSS-kwetsbaarheden die misbruik vereisen van gebruikersinteractie, zoals het openen van een kwaadaardig bestand of het bezoeken van een gemanipuleerde URL, wat kan leiden tot het uitvoeren van scripts in de context van de applicatie. Een improper access control kwetsbaarheid maakt het mogelijk voor aanvallers om zonder gebruikersinteractie willekeurige bestanden op het onderliggende systeem te lezen, waarbij toegangsbeperkingen worden omzeild. Daarnaast is er een improper input validation kwetsbaarheid die code-executie mogelijk maakt na het openen van een kwaadaardig bestand, vooral binnen administratieve netwerkzones. Ook is er een uncontrolled resource consumption kwetsbaarheid die een denial-of-service kan veroorzaken door het uitputten van systeembronnen zonder dat gebruikersinteractie nodig is. Deze kwetsbaarheden beïnvloeden verschillende aspecten van de ColdFusion-omgeving, zoals de integriteit, vertrouwelijkheid en beschikbaarheid van het systeem.

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/apsb26-119.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-21269	4.6 MEDIUM
CVE-2026-48273	9.9 CRITICAL

CVE-2026-75746	9.1 CRITICAL
CVE-2026-75993	8.5 HIGH
CVE-2026-75998	7.5 HIGH
CVE-2026-75999	8.4 HIGH
CVE-2026-76000	6.5 MEDIUM
CVE-2026-76002	6.1 MEDIUM
CVE-2026-76190	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

Getroffen producten

Adobe
ColdFusion 2023
ColdFusion 2025

Disclaimer