Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0191

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-06-2026

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 2023.19, 2025.8 en eerdere versies.

Duiding

De kwetsbaarheden betreffen onder andere improper input validation die het mogelijk maakt om zonder gebruikersinteractie willekeurige code uit te voeren. Daarnaast is er een path traversal kwetsbaarheid die, na het openen van een kwaadaardig bestand, toegang geeft tot bestanden buiten de bedoelde directorystructuur. Verder is er een incorrect authorization kwetsbaarheid die aanvallers met hoge privileges in staat stelt om op afstand willekeurige code uit te voeren en hun toegangsrechten te escaleren zonder gebruikersinteractie. Ook kunnen aanvallers met lage privileges beveiligingsmechanismen omzeilen en ongeautoriseerde lees- en schrijfacties uitvoeren. Een XML External Entity (XXE) kwetsbaarheid maakt het mogelijk om via een kwaadaardig bestand willekeurige bestanden op het systeem te lezen. Tot slot is er een stored Cross-Site Scripting (XSS) kwetsbaarheid waarbij aanvallers met lage toegangsrechten kwaadaardige JavaScript-code kunnen injecteren in formuliervelden, die bij andere gebruikers wordt uitgevoerd. Deze kwetsbaarheden zijn aanwezig in meerdere versies van Adobe ColdFusion.

Oplossingen

Adobe heeft updates uitgebracht om de kwetsbaarheden in ColdFusion versies 2023.19, 2025.8 en eerdere versies te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://helpx.adobe.com//security/products/coldfusion/apsb26-64.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-47928	5.3 MEDIUM
CVE-2026-47932	5.3 MEDIUM
CVE-2026-47929	5.1 MEDIUM
CVE-2026-47931	5.1 MEDIUM

CVE-2026-47930	**5.3 MEDIUM**
CVE-2026-47960	**5.3 MEDIUM**
CVE-2026-47933	**5.1 MEDIUM**

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-285	Improper Authorization
CWE-611	Improper Restriction of XML External Entity Reference
CWE-863	Incorrect Authorization

Getroffen producten

Adobe
ColdFusion
ColdFusion 2023
ColdFusion 2025

Disclaimer