Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0294

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-08-2026

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 2025.0.11, 2023.0.22 en eerdere versies.

Duiding

De kwetsbaarheden in Adobe ColdFusion kunnen door ongeauthenticeerde kwaadwillenden worden misbruikt om willekeurige code uit te voeren op afstand, beveiligingsmaatregelen te omzeilen, rechten te verhogen op het systeem of middels DoS de werking van de applicatie te verstoren.

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/apsb26-90.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-71384	9.6 CRITICAL
CVE-2026-48362	10.0 CRITICAL
CVE-2026-48273	9.9 CRITICAL
CVE-2026-71386	8.8 HIGH
CVE-2026-71387	8.8 HIGH
CVE-2026-71385	8.4 HIGH
CVE-2026-34635	8.4 HIGH
CVE-2026-48440	8.1 HIGH
CVE-2026-21279	8.2 HIGH

CVE-2026-25652	7.8 HIGH
CVE-2026-48386	7.5 HIGH
CVE-2026-71383	7.3 HIGH
CVE-2026-48375	6.5 MEDIUM
CVE-2026-48376	5.4 MEDIUM
CVE-2026-48384	4.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')
CWE-116	Improper Encoding or Escaping of Output
CWE-122	Heap-based Buffer Overflow
CWE-321	Use of Hard-coded Cryptographic Key
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-863	Incorrect Authorization

Getroffen producten

Adobe
ColdFusion

ColdFusion 2023
ColdFusion 2025

Disclaimer