Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0241

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-07-2026

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 meerderen kwetsbaarheden verholpen in Adobe ColdFusion versies 25.10, 23.21 en eerdere versies.

Duiding

De genoemde kwetsbaarheden kunnen leiden tot de volgende categorieen van schade:

- Willekeurig uitvoeren van code
- Onrechtmatig verhogen van privileges
- Uitlezen van willekeurige bestanden
- Omzeilen van beveiligingsmaatregelen

Adobe is op het moment van schrijven niet bewust van actief misbruik van bovengenoemde kwetsbaarheden.

Oplossingen

Adobe heeft updates beschikbaar gesteld waarin de beschreven kwetsbaarheden verholpen worden. We raden u aan de nieuwste updates te installeren. Zie de bijgevoegde referenties voor meer informatie over de kwetsbaarheden en beschikbare updates.

Referenties

› https://guides.adobe.com/coldfusion/en/docs/install-and-configure-coldfusion/coldfusion-2025-release-update-11.html
› https://helpx.adobe.com/security/products/coldfusion/apsb26-82.html

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-48327	9.0 CRITICAL
› CVE-2026-48325	9.3 CRITICAL
› CVE-2026-48324	9.1 CRITICAL
› CVE-2026-48322	9.6 CRITICAL
› CVE-2026-48321	9.3 CRITICAL

CVE-2026-48319	9.1 CRITICAL
CVE-2026-48318	9.9 CRITICAL
CVE-2026-48284	9.6 CRITICAL
CVE-2026-48320	8.5 HIGH
CVE-2026-48328	7.7 HIGH
CVE-2026-48329	2.7 LOW
CVE-2026-48332	7.7 HIGH
CVE-2026-48338	6.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-20	Improper Input Validation
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-863	Incorrect Authorization
CWE-306	Missing Authentication for Critical Function
CWE-918	Server-Side Request Forgery (SSRF)
CWE-613	Insufficient Session Expiration

Getroffen producten

Adobe
ColdFusion
ColdFusion 2023

ColdFusion
2025

Disclaimer