Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0222

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-07-2025

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 kwetsbaarheden verholpen in ColdFusion (Specifiek voor versies 25.2, 23.14, 21.20 en eerder).

Duiding

De kwetsbaarheden in ColdFusion omvatten onder andere een significante kwetsbaarheid met betrekking tot onjuiste beperking van XML External Entity Reference (XXE), hard-coded credentials, incorrecte autorisatie, XML-injectie, en verschillende soorten Cross-Site Scripting (XSS). Deze kwetsbaarheden stellen aanvallers in staat om ongeautoriseerde toegang te verkrijgen tot gevoelige informatie, privilege-escalatie uit te voeren, en schadelijke scripts in browsers van gebruikers uit te voeren. De meeste kwetsbaarheden zijn beperkt tot interne IP-adressen, wat de blootstelling kan verminderen, maar nog steeds een aanzienlijk risico vormt voor de beveiliging van de systemen. Aanvallers kunnen deze kwetsbaarheden misbruiken zonder gebruikersinteractie, wat de ernst van de situatie vergroot.

Oplossingen

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

Referenties

- https://helpx.adobe.com/security/products/coldfusion/apsb25-69.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-49535	9.3 CRITICAL
CVE-2025-49536	8.1 HIGH
CVE-2025-49537	7.9 HIGH
CVE-2025-49538	7.4 HIGH
CVE-2025-49539	6.5 MEDIUM
CVE-2025-49540	4.8 MEDIUM

CVE-2025-49541	4.8 MEDIUM
CVE-2025-49542	6.1 MEDIUM
CVE-2025-49543	4.8 MEDIUM
CVE-2025-49544	6.8 MEDIUM
CVE-2025-49545	6.8 MEDIUM
CVE-2025-49546	2.7 LOW
CVE-2025-49551	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-798	Use of Hard-coded Credentials
CWE-284	Improper Access Control
CWE-91	XML Injection (aka Blind XPath Injection)
CWE-918	Server-Side Request Forgery (SSRF)
CWE-863	Incorrect Authorization
CWE-611	Improper Restriction of XML External Entity Reference
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Getroffen producten

Adobe
ColdFusion
ColdFusion 2021

ColdFusion 2023
ColdFusion 2025

Disclaimer