



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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   |
|----------------------------------|--------------|
| ➤ <a href="#">CVE-2025-49535</a> | 9.3 CRITICAL |
| ➤ <a href="#">CVE-2025-49536</a> | 8.1 HIGH     |
| ➤ <a href="#">CVE-2025-49537</a> | 7.9 HIGH     |
| ➤ <a href="#">CVE-2025-49538</a> | 7.4 HIGH     |
| ➤ <a href="#">CVE-2025-49539</a> | 6.5 MEDIUM   |
| ➤ <a href="#">CVE-2025-49540</a> | 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   |
|-----------|--|
| > CVE-798 | Use of Hard-coded Credentials  |
| > CVE-284 | Improper Access Control  |
| > CVE-91  | XML Injection (aka Blind XPath Injection)  |
| > CVE-918 | Server-Side Request Forgery (SSRF)   |
| > CVE-863 | Incorrect Authorization  |
| > CVE-611 | Improper Restriction of XML External Entity Reference                                      |
| > CVE-79  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')       |
| > CVE-78  | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

## Getroffen producten

| Adobe              |
|--------------------|
| ColdFusion         |
| ColdFusion<br>2021 |

ColdFusion  
2023

ColdFusion  
2025

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.