Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0115

Kwetsbaarheden verholpen in Adobe ColdFusion

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-04-2025

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 2023.12, 2021.18, 2025.0 en eerder).

Duiding

De kwetsbaarheden bevinden zich in de manier waarop ColdFusion omgaat met invoervalidatie, authenticatie, toegang en deserialisatie van onbetrouwbare gegevens. Kwaadwillenden kunnen deze kwetsbaarheden misbruiken om willekeurige code uit te voeren, ongeautoriseerde toegang te verkrijgen, en gevoelige gegevens te lezen of te wijzigen. De meeste kwetsbaarheden vereisen gebruikersinteractie, zoals het openen van een kwaadaardig bestand of het bezoeken van een gecompromitteerde URL.

Oplossingen

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

Referenties

- https://helpx.adobe.com/security/products/coldfusion/apsb25-15.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-24446	8.5 HIGH
CVE-2025-30293	5.1 MEDIUM
CVE-2025-30292	5.3 MEDIUM
CVE-2025-30290	5.1 MEDIUM
CVE-2025-30288	2.0 LOW
CVE-2025-30287	2.0 LOW
CVE-2025-30286	8.6 HIGH
CVE-2025-30285	7.5 HIGH

CVE-2025-30284	7.5 HIGH
CVE-2025-30282	5.1 MEDIUM
CVE-2025-24447	6.9 MEDIUM
CVE-2025-30281	5.1 MEDIUM
CVE-2025-30294	5.3 MEDIUM
CVE-2025-30289	2.0 LOW
CVE-2025-30291	4.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-502	Deserialization of Untrusted Data
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Adobe
ColdFusion

Disclaimer