



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits d'Adobe
Numéro de Référence	59141012/25
Date de Publication	10 décembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Acrobat DC 25.001.20982 et versions antérieures
- Acrobat Reader DC 25.001.20982 et versions antérieures
- Acrobat Reader 2020 Mac - 20.005.30803 et versions antérieures
- Acrobat Reader 2020 Win - 20.005.30793 et versions antérieures
- Acrobat 2020 Mac - 20.005.30803 et versions antérieures
- Acrobat 2020 Win - 20.005.30793 et versions antérieures
- Acrobat 2024 Mac - 24.001.30273 et versions antérieures
- Acrobat 2024 Win - 24.001.30264 et versions antérieures
- Adobe DNG Software Development Kit (SDK) DNG SDK 1.7.0 et versions antérieures
- Adobe Experience Manager (AEM) AEM Cloud Service (CS)
- Adobe Experience Manager (AEM) 6.5 LTS et versions antérieures
- Adobe Experience Manager (AEM) 6.5.23 et versions antérieures
- ColdFusion 2021 Update 22 et versions antérieures
- ColdFusion 2023 Update 16 et versions antérieures
- ColdFusion 2025 Update 4 et versions antérieures
- Creative Cloud Desktop Application 6.4.0.361 et versions antérieures

Identificateurs externes

CVE-2025-64541, CVE-2025-64542, CVE-2025-64543, CVE-2025-64544, CVE-2025-64545, CVE-2025-64554, CVE-2025-64555, CVE-2025-64556, CVE-2025-64557, CVE-2025-64558, CVE-2025-64560, CVE-2025-64562, CVE-2025-64563, CVE-2025-64564, CVE-2025-64565, CVE-2025-64569, CVE-2025-64572, CVE-2025-64574, CVE-2025-64575, CVE-2025-64576, CVE-2025-64577, CVE-2025-64578, CVE-2025-

64579, CVE-2025-64580, CVE-2025-64581, CVE-2025-64582, CVE-2025-64583, CVE-2025-64585, CVE-2025-64586, CVE-2025-64590, CVE-2025-64591, CVE-2025-64592, CVE-2025-64593, CVE-2025-64594, CVE-2025-64596, CVE-2025-64597, CVE-2025-64598, CVE-2025-64599, CVE-2025-64600, CVE-2025-64601, CVE-2025-64602, CVE-2025-64603, CVE-2025-64604, CVE-2025-64605, CVE-2025-64606, CVE-2025-64607, CVE-2025-64609, CVE-2025-64610, CVE-2025-64611, CVE-2025-64612, CVE-2025-64614, CVE-2025-64615, CVE-2025-64616, CVE-2025-64619, CVE-2025-64620, CVE-2025-64622, CVE-2025-64623, CVE-2025-64626, CVE-2025-64627, CVE-2025-64789, CVE-2025-64790, CVE-2025-64791, CVE-2025-64792, CVE-2025-64793, CVE-2025-64794, CVE-2025-64796, CVE-2025-64797, CVE-2025-64799, CVE-2025-64800, CVE-2025-64801, CVE-2025-64802, CVE-2025-64803, CVE-2025-64804, CVE-2025-64808, CVE-2025-64814, CVE-2025-64817, CVE-2025-64820, CVE-2025-64821, CVE-2025-64822, CVE-2025-64823, CVE-2025-64825, CVE-2025-64826, CVE-2025-64827, CVE-2025-64829, CVE-2025-64833, CVE-2025-64839, CVE-2025-64840, CVE-2025-64841, CVE-2025-64845, CVE-2025-64847, CVE-2025-64850, CVE-2025-64852, CVE-2025-64853, CVE-2025-64857, CVE-2025-64858, CVE-2025-64860, CVE-2025-64861, CVE-2025-64863, CVE-2025-64869, CVE-2025-64875, CVE-2025-64887, CVE-2025-64888, CVE-2025-61808, CVE-2025-61809, CVE-2025-61812, CVE-2025-61822, CVE-2025-61823, CVE-2025-61811, CVE-2025-61813, CVE-2025-61821, CVE-2025-61830, CVE-2025-64897, CVE-2025-64898, CVE-2025-64546, CVE-2025-64547, CVE-2025-64548, CVE-2025-64549, CVE-2025-64550, CVE-2025-64551, CVE-2025-64552, CVE-2025-64553, CVE-2025-64559, CVE-2025-64872, CVE-2025-64873, CVE-2025-64874, CVE-2025-64881, CVE-2025-64539, CVE-2025-64540, CVE-2025-64537, CVE-2025-64783, CVE-2025-64784, CVE-2025-64893, CVE-2025-64894, CVE-2025-64786, CVE-2025-64787, CVE-2025-64785, CVE-2025-64899, CVE-2025-64896

Bilan de la vulnérabilité

Adobe a publié des mises à jour de sécurité qui permettent de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance, de contourner de mesures de sécurité, d'accéder à des données confidentielles, d'injecter du contenu dans une page d'élever ses privilèges ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité d'Adobe pour l'obtention des correctifs.

Risques

- Exécution de code arbitraire
- Accès à des informations confidentielles
- Contournement de mesures de sécurité
- Injection de contenu dans une page
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité d'Adobe:

- <https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html>
- <https://helpx.adobe.com/security/products/experience-manager/apsb25-115.html>
- <https://helpx.adobe.com/security/products/dng-sdk/apsb25-118.html>
- <https://helpx.adobe.com/security/products/acrobat/apsb25-119.html>
- <https://helpx.adobe.com/security/products/creative-cloud/apsb25-120.html>