



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits d'Adobe
Numéro de Référence	39501412/22
Date de Publication	14 Décembre 2022
Risque	Important
Impact	Important

Systemes affectés

- Adobe Campaign Classic ACC v7 version antérieures à 7.3.2
- Adobe Campaign Classic ACC v8 versions antérieures 8.4.2
- Adobe Experience Manager (AEM) Cloud Service versions antérieures à 2022.10.0
- Adobe Experience Manager (AEM) versions antérieures à 6.5.15.0
- Illustrator 2023 versions antérieures à 27.0.1
- Illustrator 2022 versions antérieures à 26.5.2

Identificateurs externes

CVE-2022-42343	CVE-2022-42351	CVE-2022-44488	CVE-2022-42345
CVE-2022-42346	CVE-2022-30679	CVE-2022-42348	CVE-2022-42349
CVE-2022-42350	CVE-2022-42352	CVE-2022-35693	CVE-2022-42354
CVE-2022-35694	CVE-2022-42356	CVE-2022-42357	CVE-2022-35695
CVE-2022-35696	CVE-2022-42360	CVE-2022-42362	CVE-2022-42364
CVE-2022-42365	CVE-2022-42366	CVE-2022-42367	CVE-2022-44462
CVE-2022-44463	CVE-2022-44465	CVE-2022-44466	CVE-2022-44467
CVE-2022-44468	CVE-2022-44469	CVE-2022-44470	CVE-2022-44471
CVE-2022-44473	CVE-2022-44474		

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, d'élever ses privilèges, de contourner des mesures de sécurité ou d'accéder à des données confidentielles

Solution

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

Risque

- Exécution de code arbitraire
- Elévation de privilèges
- Accès à des données confidentielles
- Contournement de mesures de sécurité

Référence

Bulletins de sécurité d'Adobe:

- <https://helpx.adobe.com/security/products/campaign/apsb22-58.html>
- <https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html>
- <https://helpx.adobe.com/security/products/illustrator/apsb22-60.html>