



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

## BULLETIN DE SECURITE

|                            |                                                     |
|----------------------------|-----------------------------------------------------|
| <b>Titre</b>               | Vulnérabilités affectant plusieurs produits d'Adobe |
| <b>Numéro de Référence</b> | 59951501/26                                         |
| <b>Date de Publication</b> | 15 janvier 2026                                     |
| <b>Risque</b>              | Important                                           |
| <b>Impact</b>              | Important                                           |

### Systèmes affectés

- Adobe Dreamweaver 21.6 et versions antérieures
- Adobe InDesign ID21.0 et versions antérieures
- Adobe InDesign ID19.5.5 et versions antérieures
- Illustrator 2025 29.8.3 et versions antérieures
- Illustrator 2026 30.0 et versions antérieures
- Adobe InCopy21.0 et versions antérieures
- Adobe InCopy19.5.5 et versions antérieures
- Adobe Bridge 15.1.2 (LTS) et versions antérieures
- Adobe Bridge 16.0 et versions antérieures
- Adobe Substance 3D Modeler 1.22.4 et versions antérieures
- Adobe Substance 3D Stager 3.1.5 et versions antérieures
- Adobe Substance 3D Painter 11.0.3 et versions antérieures
- Adobe Substance 3D Sampler 5.1.0 et versions antérieures
- ColdFusion 2025 Update 5 et versions antérieures
- ColdFusion 2023 Update 17 et versions antérieures
- Adobe Substance 3D Designer 15.0.3 et versions antérieures

### Identificateurs externes

|                |                |                |                |                |
|----------------|----------------|----------------|----------------|----------------|
| CVE-2026-21267 | CVE-2026-21268 | CVE-2026-21271 | CVE-2026-21272 | CVE-2026-21274 |
| CVE-2026-21275 | CVE-2026-21276 | CVE-2026-21277 | CVE-2026-21278 | CVE-2026-21280 |
| CVE-2026-21281 | CVE-2026-21283 | CVE-2026-21287 | CVE-2026-21288 | CVE-2026-21298 |
| CVE-2026-21299 | CVE-2026-21300 | CVE-2026-21301 | CVE-2026-21302 | CVE-2026-21303 |

## 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, de contourner de mesures de sécurité, d'accéder à des données confidentielles 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
- Déni de service

## Références

Bulletins de sécurité d'Adobe:

- <https://helpx.adobe.com/security/products/dreamweaver/apsb26-01.html>
- <https://helpx.adobe.com/security/products/indesign/apsb26-02.html>
- <https://helpx.adobe.com/security/products/illustrator/apsb26-03.html>
- <https://helpx.adobe.com/security/products/incopy/apsb26-04.html>
- <https://helpx.adobe.com/security/products/bridge/apsb26-07.html>
- <https://helpx.adobe.com/security/products/substance3d-modeler/apsb26-08.html>
- [https://helpx.adobe.com/security/products/substance3d\\_stager/apsb26-09.html](https://helpx.adobe.com/security/products/substance3d_stager/apsb26-09.html)
- <https://helpx.adobe.com/security/products/substance3dPainter/apsb26-10.html>
- <https://helpx.adobe.com/security/products/substance3d-sampler/apsb26-11.html>
- <https://helpx.adobe.com/security/products/coldfusion/apsb26-12.html>
- [https://helpx.adobe.com/security/products/substance3d\\_designer/apsb26-13.html](https://helpx.adobe.com/security/products/substance3d_designer/apsb26-13.html)