GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPR 9108 Port-Vila, Vanuatu
Tél : (678) 33380

1 June 2026

Avis 144 : Vulnérabilité de dépassement de tampon basé sur le tas dans Adobe Acrobat et Reader

Date de publication : 20 mai 2026
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publie l'avis suivant.

Cette alerte s'adresse aux organisations ainsi qu'aux administrateurs de systèmes et réseaux utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et des administrateurs de systèmes.

Objet de l'alerte

CVE-2009-3459 est une **vulnérabilité critique d'exécution de code à distance (RCE)** affectant **Adobe Reader** et Adobe Acrobat.

La faille est causée par un dépassement de tampon et une corruption de mémoire lors du traitement de fichiers PDF spécialement conçus, contenant du JavaScript intégré et des objets malformés.

Systèmes concernés

La vulnérabilité affecte :

- Adobe Reader 9.1 et versions antérieures
- Adobe Acrobat 9.1 et versions antérieures

Les plateformes concernées incluent :

- Microsoft Windows
- macOS
- Systèmes Linux exécutant des logiciels Adobe vulnérables.

Implications

1. **Création d'un PDF malveillant**

   - L'attaquant conçoit un PDF contenant des objets malformés ou du JavaScript malveillant.

2. **Livraison à la victime**

   - Le PDF est distribué via :
     - des courriels de phishing
     - des sites web malveillants
     - des plateformes de partage de fichiers

3. **Ouverture du PDF par la victime**

   - Le fichier est ouvert avec une version vulnérable d'Adobe Reader ou Acrobat.

4. **Déclenchement de la corruption mémoire**

   - Un mauvais traitement provoque un dépassement de tampon ou une corruption du tas en mémoire.

5. **Exécution de code à distance**

- L'attaquant exécute du code arbitraire avec les privilèges de l'utilisateur connecté.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

Appliquer les mises à jour de sécurité Adobe (Critique)

- Mettre à niveau vers des versions corrigées de :
  - **Adobe Reader**
  - **Adobe Acrobat**
- Appliquer les bulletins de sécurité Adobe publiés après 2009.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2009-3459