مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Adobe

Tracking #:432318565

Date:11-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Adobe has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Adobe has released multiple security updates addressing critical and important vulnerabilities across several products, including Adobe DNG Software Development Kit, Adobe Substance 3D Stager, Adobe Premiere Pro, Adobe Illustrator, Adobe Acrobat, Adobe Acrobat Reader, Adobe Commerce, Adobe Commerce B2B, and Magento Open Source. These updates resolve issues that could lead to arbitrary code execution, privilege escalation, or other security impacts.

Affected Products and Notable Vulnerabilities:

1. Adobe DNG Software Development Kit (SDK)
Fixed Version: DNG SDK **1.7.1 build 2502**
Critical (CVSS 7.8) – Arbitrary Code Execution

- **CVE-2026-27280:** Out-of-bounds Write (**CWE-787**)

Important (CVSS 5.5) – Application Denial-of-Service

- **CVE-2026-27281:** Integer Overflow or Wraparound (**CWE-190**)

2. Adobe Substance 3D Stager
Fixed Version: 3.1.8
Critical (CVSS 7.8) – Arbitrary Code Execution

- **CVE-2026-27273:** Out-of-bounds Write (**CWE-787**)
- **CVE-2026-27274:** Out-of-bounds Write (**CWE-787**)
- **CVE-2026-27275:** Out-of-bounds Write (**CWE-787**)
- **CVE-2026-27276:** Use After Free (**CWE-416**)
- **CVE-2026-27277:** Use After Free (**CWE-416**)
- **CVE-2026-27279:** Out-of-bounds Write (**CWE-787**)

3. Adobe Premiere Pro
Fixed Versions:

- **Premiere Pro 26.0**
- **Premiere Pro 25.6 LTS**

Critical (CVSS 7.8) – Arbitrary Code Execution

- **CVE-2026-27269:** Out-of-bounds Read (**CWE-125**)

4. Adobe Illustrator
Fixed Versions:

- **Illustrator 2025 – 29.8.5 and later**
- **Illustrator 2026 – 30.2 and later**

Critical (CVSS 8.6) – Arbitrary Code Execution

- **CVE-2026-21333:** Untrusted Search Path (**CWE-426**)

Critical (CVSS 7.8) – Arbitrary Code Execution

- **CVE-2026-21362:** Out-of-bounds Write (**CWE-787**)
- **CVE-2026-27271:** Heap-based Buffer Overflow (**CWE-122**)
- **CVE-2026-27272:** Out-of-bounds Write (**CWE-787**)

- **CVE-2026-27267:** Stack-based Buffer Overflow (**CWE-121**)

Important (CVSS 5.5) – Memory Exposure / DoS

- **CVE-2026-27268:** Out-of-bounds Read (**CWE-125**) – Memory Exposure
- **CVE-2026-27270:** Out-of-bounds Read (**CWE-125**) – Arbitrary code execution

5. Adobe Acrobat & Acrobat Reader

Fixed Versions:

- **Acrobat DC / Reader DC:** 25.001.21288
- **Acrobat 2024:** 24.001.30356

Critical (CVSS 7.8) – Arbitrary Code Execution

- **CVE-2026-27220:** Use After Free (**CWE-416**)
- **CVE-2026-27278:** Use After Free (**CWE-416**)

Important (CVSS 5.5) – Privilege Escalation

- **CVE-2026-27221:** Improper Verification of Cryptographic Signature (**CWE-347**)

6. Adobe Commerce / Magento Open Source – CVE Details

Fixed Versions

Adobe Commerce

- 2.4.9-beta1 (for 2.4.9-alpha3)
- 2.4.8-p4 (for 2.4.8-p3 and earlier)
- 2.4.7-p9 (for 2.4.7-p8 and earlier)
- 2.4.6-p14 (for 2.4.6-p13 and earlier)
- 2.4.5-p16 (for 2.4.5-p15 and earlier)
- 2.4.4-p17 (for 2.4.4-p16 and earlier)

Adobe Commerce B2B

- 1.5.3-beta1
- 1.5.2-p4
- 1.4.2-p9
- 1.3.5-p14
- 1.3.4-p16
- 1.3.3-p17

Magento Open Source

- 2.4.9-beta1
- 2.4.8-p4
- 2.4.7-p9
- 2.4.6-p14
- 2.4.5-p16

Critical Vulnerabilities

Critical (CVSS 8.7) – Privilege Escalation

- **CVE-2026-21290:** Stored Cross-Site Scripting (**CWE-79**)

Critical (CVSS 8.1) – Privilege Escalation

- **CVE-2026-21361:** Stored Cross-Site Scripting (**CWE-79**)
- **CVE-2026-21284:** Stored Cross-Site Scripting (**CWE-79**)

Critical (CVSS 8.0) – Privilege Escalation

- **CVE-2026-21311:** Stored Cross-Site Scripting (**CWE-79**)

Critical (CVSS 7.5) – Security Feature Bypass / Privilege Escalation

- **CVE-2026-21289:** Incorrect Authorization (**CWE-863**)
- **CVE-2026-21309:** Incorrect Authorization (**CWE-863**)

Important Vulnerabilities
Important (CVSS 6.8) – Security Feature Bypass

- **CVE-2026-21360:** Path Traversal (**CWE-22**)

Important (CVSS 5.5) – Arbitrary File System Read / Security Bypass

- **CVE-2026-21293:** Server-Side Request Forgery (**CWE-918**)
- **CVE-2026-21294:** Server-Side Request Forgery (**CWE-918**)

Important (CVSS 5.4) – Arbitrary Code Execution

- **CVE-2026-21292:** Stored Cross-Site Scripting (**CWE-79**)

Important (CVSS 5.3) – Security Feature Bypass / DoS

- **CVE-2026-21286:** Incorrect Authorization (**CWE-863**)
- **CVE-2026-21282:** Improper Input Validation (**CWE-20**) – Application DoS
- **CVE-2026-21310:** Improper Input Validation (**CWE-20**)

Important (CVSS 4.8) – Arbitrary Code Execution

- **CVE-2026-21291:** Stored Cross-Site Scripting (**CWE-79**)

Important (CVSS 4.7) – Security Feature Bypass

- **CVE-2026-21359:** Incorrect Authorization (**CWE-863**)

Important (CVSS 4.3) – Security Feature Bypass

- **CVE-2026-21285:** Incorrect Authorization (**CWE-863**)

Moderate Vulnerabilities
Moderate (CVSS 3.5) – Security Feature Bypass

- **CVE-2026-21296:** Incorrect Authorization (**CWE-863**)
- **CVE-2026-21297:** Incorrect Authorization (**CWE-863**)

Moderate (CVSS 3.1) – Security Feature Bypass

- **CVE-2026-21295:** Open Redirect (**CWE-601**)

Note:
Refer to the official Adobe Security Bulletins for the full list of CVEs, fixed versions, and additional information.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Adobe.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://helpx.adobe.com/security/products/dng-sdk/apsb26-30.html
- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb26-28.html
- https://helpx.adobe.com/security/products/acrobat/apsb26-26.html
- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html
- https://helpx.adobe.com/security/products/magento/apsb26-05.html