مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Adobe January 2026 Security Updates
Tracking #:432318251
Date:15-01-2026

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Adobe has released January 2026 Patch Tuesday security updates addressing 25 vulnerabilities across 11 products, including multiple critical arbitrary code execution flaws.

TECHNICAL DETAILS:

Adobe has released January 2026 Patch Tuesday security updates addressing 25 vulnerabilities across 11 products, including multiple critical arbitrary code execution flaws. The most severe issue (CVE-2025-66516, CVSS 10.0) affects ColdFusion through a vulnerable Apache Tika dependency, enabling remote code execution (RCE) via malicious PDF/XFA content. While no active exploitation has been observed, Adobe has assigned a Priority 1 rating to ColdFusion updates, indicating high risk and urgent remediation requirements. Other products (Dreamweaver, InDesign, Illustrator, Bridge, InCopy, and Substance 3D suite) received Priority 3 updates, primarily mitigating code execution, memory corruption, and DoS risks.

Vulnerability Details (Consolidated)
ColdFusion (Priority 1 – Immediate Action Required)
- **CVE-2025-66516**
  - **Type**: XML External Entity (XXE) via Apache Tika
  - **CVSS**: 10.0 (Critical)
  - **Impact**:
    - Remote Code Execution
    - SSRF
    - Information disclosure
    - Denial-of-Service
  - **Affected**:
    - ColdFusion 2025 Update 5 and earlier
    - ColdFusion 2023 Update 17 and earlier
  - **Fixed In**:
    - ColdFusion 2025 Update 6
    - ColdFusion 2023 Update 18

Dreamweaver (APSB26-01)
- **Severity**: Critical
- **Key CVEs**:
  - CVE-2026-21267 – OS Command Injection → RCE
  - CVE-2026-21268 – Input Validation → RCE
  - CVE-2026-21271 – Input Validation → RCE
  - CVE-2026-21272 – Arbitrary File Write
  - CVE-2026-21274 – Authorization Bypass → RCE
- **Fix**: Version 21.7

InDesign (APSB26-02)
- **Severity**: Critical / Important
- **Key CVEs**:
  - CVE-2026-21275 / 21276 – Uninitialized Pointer → RCE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

- o CVE-2026-21277 / 21304 – Heap Buffer Overflow → RCE
- o CVE-2026-21278 – Out-of-Bounds Read → Memory Exposure
- **Fix**: ID21.1 / ID20.5.1

Illustrator (APSB26-03)
- **Severity**: Critical / Important
- **Key CVEs**:
    - o CVE-2026-21280 – Untrusted Search Path → RCE
    - o CVE-2026-21288 – NULL Pointer Dereference → DoS
- **Fix**: 29.8.4+ / 30.1+

InCopy (APSB26-04)
- **Severity**: Critical
- **CVE**:CVE-2026-21281 – Heap Buffer Overflow → RCE
- **Fix**: 21.1 / 20.5.1

Bridge (APSB26-07)
- **Severity**: Critical
- **CVE**:CVE-2026-21283 – Heap Buffer Overflow → RCE
- **Fix**: 15.1.3 (LTS) / 16.0.1

Substance 3D Products
Modeler
- CVE-2026-21298 / 21299 – Out-of-Bounds Write → RCE
- CVE-2026-21300 / 21301 – NULL Dereference → DoS
- CVE-2026-21302 / 21303 – Out-of-Bounds Read → Memory Exposure
Stager
- CVE-2026-21287 – Use-After-Free → RCE
Painter
- CVE-2026-21305 – Out-of-Bounds Write → RCE
Sampler
- CVE-2026-21306-Critical RCE
Designer
- CVE-2026-21308 – Out-of-Bounds Read → Memory Leak

RECOMMENDATIONS:

- Apply all Adobe January 2026 security updates without exception.
- Prioritize remediation in the following order:
    - o ColdFusion (Priority 1)
    - o All Critical RCE client-side products
    - o Remaining high/medium severity products

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.

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

REFERENCES:

- https://helpx.adobe.com/security.html