

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Adobe**

Tracking #:432318119

Date:10-12-2025

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 INTELLIGENCE 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 its December 2025 security updates to address multiple vulnerabilities in Adobe ColdFusion, Adobe Experience Manager, Adobe DNG SDK, Adobe Acrobat Reader, and Adobe Creative Cloud Desktop. These updates resolve critical and important vulnerabilities that could lead to arbitrary code execution, privilege escalation, memory corruption, security feature bypass, or denial-of-service.

### Affected Products and Key Vulnerabilities:

#### 1. Adobe ColdFusion

- Arbitrary code execution via unrestricted file upload, deserialization of untrusted data, and improper input validation.
- Arbitrary file system read through XML External Entity (XXE) vulnerability.
- **Severity:** Critical (CVSS 8.2–9.1)
- **CVE Numbers:** CVE-2025-61808, CVE-2025-61809, CVE-2025-61810, CVE-2025-61811, CVE-2025-61812, CVE-2025-61813

#### 2. Adobe Experience Manager (AEM)

- Arbitrary code execution via DOM-based Cross-Site Scripting (XSS).
- Arbitrary file system read due to dependency on vulnerable third-party component.
- **Severity:** Critical (CVSS 8.5–9.3)
- **CVE Numbers:** CVE-2025-64537, CVE-2025-64539, CVE-2025-64540

#### 3. Adobe DNG Software Development Kit (SDK)

- Arbitrary code execution via integer overflow/wraparound.
- Memory exposure via heap-based buffer overflow and out-of-bounds read.
- **Severity:** Critical (CVSS 7.1–7.8)
- **CVE Numbers:** CVE-2025-64783, CVE-2025-64784, CVE-2025-64893

#### 4. Adobe Acrobat and Reader

- Arbitrary code execution and memory exposure vulnerabilities.
- **Severity:** Critical (CVSS 7.1–7.8)
- **CVE Numbers:** CVE-2025-64783, CVE-2025-64784, CVE-2025-64893

#### 5. Adobe Creative Cloud Desktop Application

- Application denial-of-service due to creation of temporary files with incorrect permissions.
- **Severity:** Important (CVSS 5)
- **CVE Number:** CVE-2025-64896

### Impact:

Exploitation of these vulnerabilities could allow attackers to execute arbitrary code, access sensitive information, bypass security controls, or cause denial-of-service conditions.

### 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/security-bulletin.html>