مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Adobe June 2026 Security Updates

Tracking #:432319109

Date:11-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Adobe has released its June 2026 Security Updates addressing 123 vulnerabilities across 11 product families.

TECHNICAL DETAILS:

Adobe has released its June 2026 Security Updates addressing 123 vulnerabilities across 11 product families, including Adobe Acrobat Reader, ColdFusion, Experience Manager (AEM), Experience Manager Forms, InDesign, InCopy, Dreamweaver, Substance 3D Sampler, Content Credentials SDK, Format Plugins, and Campaign Classic.
Of particular concern are two critical vulnerabilities in Adobe Campaign Classic (ACC), CVE-2026-48303 and CVE-2026-47938, both assigned a CVSS score of 10.0, the highest possible severity rating. Successful exploitation could allow unauthenticated remote attackers to achieve arbitrary code execution.
Adobe has stated that no active exploitation has been observed at the time of release; however, organizations should prioritize remediation due to the severity of the vulnerabilities and the potential for rapid weaponization.

Critical Vulnerability Details

1. **CVE-2026-48303- Adobe Campaign Classic**
   - Severity: Critical
   - CVSS Score: 10.0
   - CWE: CWE-863 (Incorrect Authorization)
   - Impact: Arbitrary Code Execution
2. **CVE-2026-47938- Adobe Campaign Classic**
   - Severity: Critical
   - CVSS Score: 10.0
   - CWE: CWE-863 (Incorrect Authorization)
   - Impact: Arbitrary Code Execution
3. **CVE-2026-47928 – Adobe ColdFusion Remote Code Execution Vulnerability**
   - **Severity:** Critical
   - **CVSS Score:** 9.6
   - CWE:CWE-79 Cross-site Scripting (Stored XSS)
   - **Impact:** Arbitrary Code Execution
4. **CVE-2026-34691 – Adobe Experience Manager Forms Stored Cross-Site Scripting (XSS) Vulnerability**
   - Severity: Critical
   - CVSS Score: 9.3
   - CWE: CWE-79-Vulnerability Type: Stored Cross-Site Scripting (XSS)

Note: Refer to the Adobe June 2026 release notes for the full list of CVEs and additional information.

Affected Products:
Adobe Campaign Classic

- ACC v7: 7.4.3 build 9394 and earlier versions

Adobe ColdFusion
- ColdFusion 2025 Update 8 and earlier
- ColdFusion 2023 Update 19 and earlier

Adobe Acrobat and Acrobat Reader
- Acrobat 26.001.21651 and earlier
- Acrobat Reader 26.001.21651 and earlier
- Acrobat 2024 24.001.30365 and earlier

Adobe Experience Manager (AEM)
- AEM Cloud Service (CS)
- AEM 6.5 LTS SP1 and earlier
- AEM SP24 and earlier
- AEM 6.5.24.0 and earlier

Adobe Experience Manager Forms
- Supported vulnerable versions per APSB26-57

Adobe InDesign
- ID21.3 and earlier
- ID20.5.3 and earlier

Adobe InCopy
- 21.3 and earlier
- 20.5.3 and earlier

Adobe Dreamweaver
- 21.7 and earlier

Adobe Substance 3D Sampler
- 6.0.0 and earlier

Content Credentials SDK
- JS SDK @contentauth/c2pa-web@0.7.1 and earlier
- Rust SDK c2pa-v0.80.1 and earlier

Adobe Format Plugins
- 1.1.2 and earlier

RECOMMENDATIONS:

- Apply Adobe's June 2026 security updates as a matter of priority.
- Prioritize remediation of Campaign Classic and ColdFusion deployments

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.html