مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in Adobe ColdFusion

Tracking #:432319231

Date:02-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Adobe has released security updates for Adobe ColdFusion 2025 and Adobe ColdFusion 2023 to address multiple critical and important vulnerabilities.

TECHNICAL DETAILS:

Adobe has released Priority 1 security updates for Adobe ColdFusion 2025 and Adobe ColdFusion 2023 to address multiple critical and important vulnerabilities. The flaws could allow attackers to perform unauthenticated remote code execution (RCE), privilege escalation, arbitrary file system read, and security feature bypass. Several of the vulnerabilities carry the maximum CVSS v3.1 score of 10.0, indicating they can be exploited remotely with little complexity and may result in complete compromise of affected servers.
Adobe has stated that there is currently no evidence of active exploitation in the wild. However, due to the critical nature of these vulnerabilities and the exposure of ColdFusion servers to the internet, organizations should prioritize immediate patching.

Critical Vulnerabilities:

- CVE-2026-48276
  - Type: Unrestricted Upload of File with Dangerous Type (CWE-434)
  - Impact: Arbitrary Code Execution
  - CVSS: 10.0 (Critical)
  - Allows attackers to upload malicious files that can be executed on the server.
- CVE-2026-48277
  - Type: Improper Input Validation (CWE-20)
  - Impact: Arbitrary Code Execution
  - CVSS: 10.0 (Critical)
  - Improper validation of user input may allow remote execution of attacker-controlled code.
- CVE-2026-48281
  - Type: Improper Input Validation (CWE-20)
  - Impact: Arbitrary Code Execution
  - CVSS: 10.0 (Critical)
  - A specially crafted request may lead to remote code execution.
- CVE-2026-48316
  - Type: Improper Input Validation (CWE-20)
  - Impact: Arbitrary Code Execution
  - CVSS: 10.0 (Critical)
  - Successful exploitation enables execution of arbitrary code on the vulnerable server.
- CVE-2026-48282
  - Type: Path Traversal (CWE-22)
  - Impact: Arbitrary Code Execution
  - CVSS: 10.0 (Critical)
  - Path traversal can be leveraged to execute malicious code outside intended directories.
- CVE-2026-48283
  - Type: Unrestricted Upload of File with Dangerous Type (CWE-434)
  - Impact: Arbitrary Code Execution

- CVSS: 10.0 (Critical)
- Allows upload and execution of malicious files leading to complete server compromise.

- CVE-2026-48313
  - Type: Path Traversal (CWE-22)
  - Impact: Arbitrary File System Read
  - CVSS: 9.3 (Critical)
  - May allow attackers to read sensitive files from the server.
- CVE-2026-48315
  - Type: Improper Input Validation (CWE-20)
  - Impact: Privilege Escalation
  - CVSS: 9.3 (Critical)
  - Could enable attackers to obtain elevated privileges within the application.
- CVE-2026-48307
  - Type: Reflected Cross-Site Scripting (CWE-79)
  - Impact: Arbitrary Code Execution
  - CVSS: 8.8 (Critical)
  - Exploitation requires user interaction and may facilitate execution of malicious code.
- CVE-2026-48285
  - Type: Server-Side Request Forgery (SSRF) (CWE-918)
  - Impact: Security Feature Bypass
  - CVSS: 8.6 (Critical)
  - May allow attackers to bypass security controls and access internal resources.

Important Vulnerability

- CVE-2026-48314
  - Type: Path Traversal (CWE-22)
  - Impact: Privilege Escalation
  - Severity: Important
  - CVSS: 6.5
  - May allow attackers to elevate privileges through directory traversal techniques.

Affected Products:

Product	Affected Versions	Fixed Version
Adobe ColdFusion 2025	Update 9 and earlier	Update 10
Adobe ColdFusion 2023	Update 20 and earlier	Update 21

RECOMMENDATIONS:

Immediate Actions:

- Immediately upgrade ColdFusion 2025 & ColdFusion 2023 to fixed version.
- Prioritize patching internet-facing ColdFusion servers.

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/uk/security/products/coldfusion/apsb26-68.html