مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - Adobe

Tracking #:432318794

Date:15-04-2026

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 security updates addressing multiple vulnerabilities across several products, including Acrobat Reader, InDesign, InCopy, Experience Manager, FrameMaker, Connect, ColdFusion, Bridge, Photoshop, DNG SDK, and Illustrator.

These vulnerabilities could allow attackers to execute arbitrary code, access sensitive data, bypass security controls, or cause denial-of-service (DoS) conditions.

Vulnerability Details

Adobe Acrobat Reader

- **CVE-2026-34622** – Critical (Prototype Pollution): Arbitrary code execution
- **CVE-2026-34626** – Important (Prototype Pollution): Arbitrary file system read

Adobe InDesign

- **CVE-2026-27283, CVE-2026-27284, CVE-2026-27291, CVE-2026-34627, CVE-2026-34628, CVE-2026-34629, CVE-2026-27238** – Critical: Arbitrary code execution
- **CVE-2026-27285** – Important: Denial-of-service
- **CVE-2026-27286** – Important: Memory exposure

Adobe InCopy

- **CVE-2026-27287, CVE-2026-34631** – Critical: Arbitrary code execution

Adobe Experience Manager (AEM)

- **CVE-2026-27288, CVE-2026-34623, CVE-2026-34624, CVE-2026-34625** – Important: Cross-site scripting (XSS) leading to code execution

Adobe FrameMaker

- Multiple Critical vulnerabilities (**CVE-2026-27290 to CVE-2026-27298**) enabling arbitrary code execution
- **CVE-2026-27299** – Important: File system read
- **CVE-2026-27300, CVE-2026-27301** – Important: Memory exposure

Adobe Connect

- **CVE-2026-27302, CVE-2026-27303, CVE-2026-34615** – Critical: Deserialization leading to code execution
- **CVE-2026-27243, CVE-2026-27245, CVE-2026-27246** – Critical: XSS leading to code execution
- **CVE-2026-34617** – Critical: Privilege escalation
- **CVE-2026-21331, CVE-2026-34614** – Important: XSS

Adobe ColdFusion

- **CVE-2026-34619, CVE-2026-27305** – Critical: Path traversal
- **CVE-2026-27304, CVE-2026-27306** – Critical: Arbitrary code execution
- **CVE-2026-27282** – Critical: Security bypass
- **CVE-2026-27307, CVE-2026-27308** – Moderate: Denial-of-service

Adobe Bridge

- **CVE-2026-34630, CVE-2026-27310, CVE-2026-27311, CVE-2026-27312, CVE-2026-27313** – Critical: Arbitrary code execution
- **CVE-2026-27222** – Important: Denial-of-service

Adobe Photoshop

- **CVE-2026-27289** – Critical: Arbitrary code execution

Adobe DNG SDK

- **CVE-2026-27258, CVE-2026-27259** – Important: Denial-of-service
- **CVE-2026-27260** – Important: Memory exposure

Adobe Illustrator

- **CVE-2026-34618** – Critical: Arbitrary code execution

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