مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Adobe

Tracking #:432317692

Date:11-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Adobe released security bulletins for a number of its products, disclosing multiple vulnerabilities ranging from important to critical severity.

TECHNICAL DETAILS:

Adobe released security bulletins for a number of its products, disclosing multiple vulnerabilities ranging from important to critical severity. Several of these vulnerabilities could allow arbitrary code execution, security feature bypass, remote code execution, input validation issues, or unauthorized filesystem writes. Notably, Adobe ColdFusion, Substance 3D Modeler, Experience Manager, and Acrobat/Reader, among others, are among the affected products.
Organizations using these Adobe products are advised to prioritize patching, configuration hardening, and risk mitigation to prevent attacks.

Product	CVE(s)	Vulnerability Type	Potential Impact
Acrobat & Reader	CVE-2025-54257	Use After Free	Arbitrary code execution / crash
	CVE-2025-54255	Violation of Secure Design Principles	Security bypass, privilege escalation
After Effects	CVE-2025-54239, CVE-2025-54240, CVE-2025-54241	Out-of-bounds Read	Information disclosure, memory corruption
Premiere Pro	CVE-2025-54242	Use After Free	Arbitrary code execution
Commerce (Magento)	CVE-2025-54236	Improper Input Validation	Injection / logic manipulation
Substance 3D Viewer	CVE-2025-54243, CVE-2025-54245	Out-of-bounds Write	Code execution, memory corruption
	CVE-2025-54244	Heap-based Buffer Overflow	Code execution
Experience Manager (AEM)	CVE-2025-54248, CVE-2025-54247, CVE-2025-54250	Improper Input Validation	Security feature bypass
	CVE-2025-54246	Incorrect Authorization	Privilege escalation / unauthorized access
	CVE-2025-54249	Server-Side Request Forgery (SSRF)	Internal network access, data exfiltration
	CVE-2025-54251	XML Injection / Blind XPath Injection	Data manipulation / disclosure
	CVE-2025-54252	Stored Cross-Site Scripting (XSS)	Persistent client-side compromise
Dreamweaver	CVE-2025-54256	Cross-Site Request Forgery (CSRF)	Unauthorized actions on behalf of a user
Substance 3D Modeler	CVE-2025-54258	Use After Free	Arbitrary code execution
	CVE-2025-54259	Integer Overflow / Wraparound	Memory corruption, crash
	CVE-2025-54260	Out-of-bounds Read	Information disclosure
ColdFusion	CVE-2025-54261	Path Traversal	Arbitrary file write / directory escape

Affected Products:

- Acrobat DC Win - 25.001.20672 and earlier versions
- Acrobat DCMac - 25.001.20668 and earlier versions
- Acrobat Reader DC Win - 25.001.20672 and earlier versions
- Acrobat Reader DC Mac - 25.001.20668 and earlier versions
- Acrobat 2024 Win & Mac - 24.001.30254 and earlier versions
- Acrobat 2020 Win & Mac - 20.005.30774 and earlier versions
- Acrobat Reader 2020 Win & Mac - 20.005.30774 and earlier versions
- Adobe After Effects 24.6.7 and earlier versions
- Adobe After Effects 25.3 and earlier versions
- Adobe Premiere Pro 25.3 and earlier versions
- Adobe Premiere Pro 24.6.5 and earlier versions
- Adobe Commerce 2.4.9-alpha2 and earlier versions
- Adobe Commerce 2.4.8-p2 and earlier versions
- Adobe Commerce 2.4.7-p7 and earlier versions
- Adobe Commerce 2.4.6-p12 and earlier versions
- Adobe Commerce 2.4.5-p14 and earlier versions
- Adobe Commerce 2.4.4-p15 and earlier versions
- Adobe Commerce B2B 1.5.3-alpha2 and earlier versions
- Adobe Commerce B2B 1.5.2-p2 and earlier versions
- Adobe Commerce B2B 1.4.2-p7 and earlier versions
- Adobe Commerce B2B 1.3.4-p14 and earlier versions
- Adobe Commerce B2B 1.3.3-p15 and earlier versions
- Magento Open Source 2.4.9-alpha2 and earlier versions
- Magento Open Source 2.4.8-p2 and earlier versions
- Magento Open Source 2.4.7-p7 and earlier versions
- Magento Open Source 2.4.6-p12 and earlier versions
- Magento Open Source 2.4.5-p14 and earlier versions
- Adobe Substance 3D Viewer 0.25.1 and earlier versions
- AEM Cloud Service (CS) 6.5 LTS SP1 and earlier versions
- AEM Cloud Service (CS) 6.5.23 and earlier versions
- Adobe Dreamweaver 21.5 and earlier versions
- Adobe Substance 3D Modeler 1.22.2 and earlier versions
- ColdFusion 2025 Update 3 and earlier versions
- ColdFusion 2023 Update 15 and earlier versions
- ColdFusion 2021 Update 21 and earlier versions

RECOMMENDATIONS:

Apply Security Updates Immediately

- Refer to the official Adobe Security Bulletins for each product and install the latest patches without delay.

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/products/coldfusion/apsb25-93.html
- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-92.html
- https://helpx.adobe.com/security/products/dreamweaver/apsb25-91.html
- https://helpx.adobe.com/security/products/experience-manager/apsb25-90.html
- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-89.html
- https://helpx.adobe.com/security/products/magento/apsb25-88.html
- https://helpx.adobe.com/security/products/premiere_pro/apsb25-87.html
- https://helpx.adobe.com/security/products/acrobat/apsb25-85.html