مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Adobe Experience Manager (AEM) Flaw Under Active Exploitation

Tracking #:432317823

Date:16-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability has been identified in Adobe Experience Manager (AEM), tracked as CVE-2025-54253, which is under active exploitation in the wild.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability has been identified in Adobe Experience Manager (AEM), tracked as CVE-2025-54253, which is under active exploitation in the wild. This flaw impacts Adobe Experience Manager Forms versions 6.5.23 and earlier and has been assigned a CVSS base score of 10.0, indicating the highest level of severity.
The vulnerability stems from a misconfiguration weakness that allows unauthenticated attackers to bypass built-in security mechanisms and execute arbitrary code on affected systems without any user interaction.
Security researchers have confirmed that public proof-of-concept (PoC) exploits for CVE-2025-54253 and a related vulnerability (CVE-2025-54254) are now available online. Active exploitation campaigns have been observed targeting exposed AEM instances, particularly those accessible from the internet.
Due to the extensive use of AEM for web content management, customer engagement portals, and document workflows, exploitation could lead to complete system compromise, data theft, or deployment of ransomware and botnet payloads.
Organizations are strongly advised to apply the latest security patches immediately

1. **CVE-2025-54253 — Struts Dev Mode Configuration Issue- Remote Code Execution- Critical 10.0**
   - **Description:** A Misconfiguration vulnerability that could result in arbitrary code execution. An attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.
   - **Impact:** Could lead to remote command execution or information disclosure.
   - **Severity:** Critical; active exploitation observed.

2. **CVE-2025-49533**
   - **Description:** A flaw in the GetDocumentServlet component allows remote, unauthenticated code execution.
   - **Attack Vector:** Network-based, unauthenticated requests.
   - **Impact:** Attackers can execute arbitrary Java code on the affected server.

3. **CVE-2025-54254 — XML External Entity (XXE)**
   - **Description:** Improper handling of XML input allows processing of external entities.
   - **Impact:** Attackers can access sensitive files or internal resources via crafted XML payloads.

Affected Product Versions:

- Adobe Experience Manager (AEM) Forms on JEE 6.5.23.0 and earlier

Fixed Version:

- Adobe Experience Manager (AEM) Forms on JEE 6.5.0-0108

RECOMMENDATIONS:

- Apply Security Patches: Upgrade Adobe Experience Manager Forms version to fixed version or later as released in Adobe's October 2025 security updates.

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/aem-forms/apsb25-82.html