Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Adobe Patches Three Critical Flaws in AEM Forms on JEE

Date of Publication

August 6, 2025

Admiralty Code

A1

TA Number

TA2025240

Summary

First Seen: April 2025
Affected Product: Adobe Experience Manager (MS)
Impact: In August 2025, Adobe patched three critical vulnerabilities (CVE-2025-49533, CVE-2025-54253, CVE-2025-54254) in AEM Forms on JEE that allowed remote code execution and arbitrary file access. These flaws, some with CVSS scores up to 10, had been disclosed months earlier but were only addressed after public exploit details emerged. Organizations are urged to apply the emergency updates immediately to mitigate these severe security risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-49533	Adobe Experience Manager (MS) Remote Code Execution Vulnerability	Adobe Experience Manager (MS)	✗	✗	✓
CVE-2025-54253	Adobe Experience Manager (MS) Misconfiguration Vulnerability	Adobe Experience Manager (MS)	✗	✗	✓
CVE-2025-54254	Adobe Experience Manager (MS) Improper Restriction of XML External Entity Vulnerability	Adobe Experience Manager (MS)	✗	✗	✓

Vulnerability Details

#1 In August 2025, Adobe released emergency patches addressing three critical vulnerabilities in Adobe Experience Manager (AEM) Forms on JEE, affecting version 6.5.23.0 and earlier. These vulnerabilities, CVE-2025-49533, CVE-2025-54253, and CVE-2025-54254, pose severe risks including unauthenticated remote code execution and arbitrary file read capabilities. They were reported to Adobe as early as April 2025, but some remained unpatched until proof-of-concept exploits were publicly released.

#2 CVE-2025-49533 is the most severe, involving insecure deserialization that allows remote code execution without authentication or user interaction. With a CVSS score of 9.8, it presents a significant threat to unpatched systems. Adobe addressed this flaw in July 2025 as part of a scheduled security update, but concerns were raised due to the long delay between disclosure and patch availability.

#3 The two remaining vulnerabilities, CVE-2025-54253 and CVE-2025-54254, were patched in an emergency update on August 5, 2025, after security researchers publicly shared technical details. CVE-2025-54253 allows arbitrary code execution via misconfigurations, while CVE-2025-54254 is a critical XML External Entity (XXE) vulnerability with a CVSS score of 10, enabling attackers to read arbitrary files on the server.

#4 Organizations using AEM Forms on JEE are urged to immediately apply the latest patches, review system configurations, and harden their XML parsing environments. Failure to act leaves systems vulnerable to exploitation, especially given the public availability of exploit code.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-49533	Adobe Experience Manager (AEM) Forms on JEE version 6.5.23.0 and earlier	cpe:2.3:a:adobe:experience_manager:*:*:*:*:*:*:*:*	CWE-502
CVE-2025-54253			CWE-16
CVE-2025-54254			CWE-611

Recommendations

Apply Security Patches Immediately: Upgrade AEM Forms on JEE to the latest patched versions as provided by Adobe. Ensure the emergency August 5, 2025 patch for CVE-2025-54253 and CVE-2025-54254 is installed.

Harden Configuration Settings: Disable unused or unnecessary servlets and endpoints to minimize the attack surface. Review access controls and ensure only authenticated users can access administrative or sensitive resources. Use network-level restrictions (e.g., firewall rules, reverse proxies) to isolate AEM Forms on JEE from untrusted environments.

Secure XML Parsing: Prevent XXE attacks (CVE-2025-54254) by disabling support for external entities in XML parsers. Validate and sanitize all XML inputs and configure XML libraries securely.

Conduct Vulnerability Scanning & Monitoring: Perform internal scans using tools like Nessus, Qualys, or Burp Suite to detect signs of exploitation. Monitor system logs and network activity for indicators of compromise, especially related to deserialization or XML processing anomalies.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0042** Resource Development	**TA0001** Initial Access	**TA0004** Privilege Escalation
TA0007 Discovery	**T1068** Exploitation for Privilege Escalation	**T1190** Exploit Public-Facing Application	**T1083** File and Directory Discovery
T1588.005 Exploits	**T1588** Obtain Capabilities	**T1059** Command and Scripting Interpreter	**T1588.006** Vulnerabilities

Patch Details

CVE-2025-49533: Fixed in AEM Forms on JEE 6.5.0.0.20250527.0 (Released July 2025)
CVE-2025-54253 & CVE-2025-54254: Fixed in AEM Forms on JEE 6.5.0-0108

Links:
https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html

https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

References

https://experienceleague.adobe.com/en/docs/experience-manager-65/content/forms/troubleshooting/mitigating-xxe-and-configuration-vulnerabilities-for-experience-manager-forms-jee

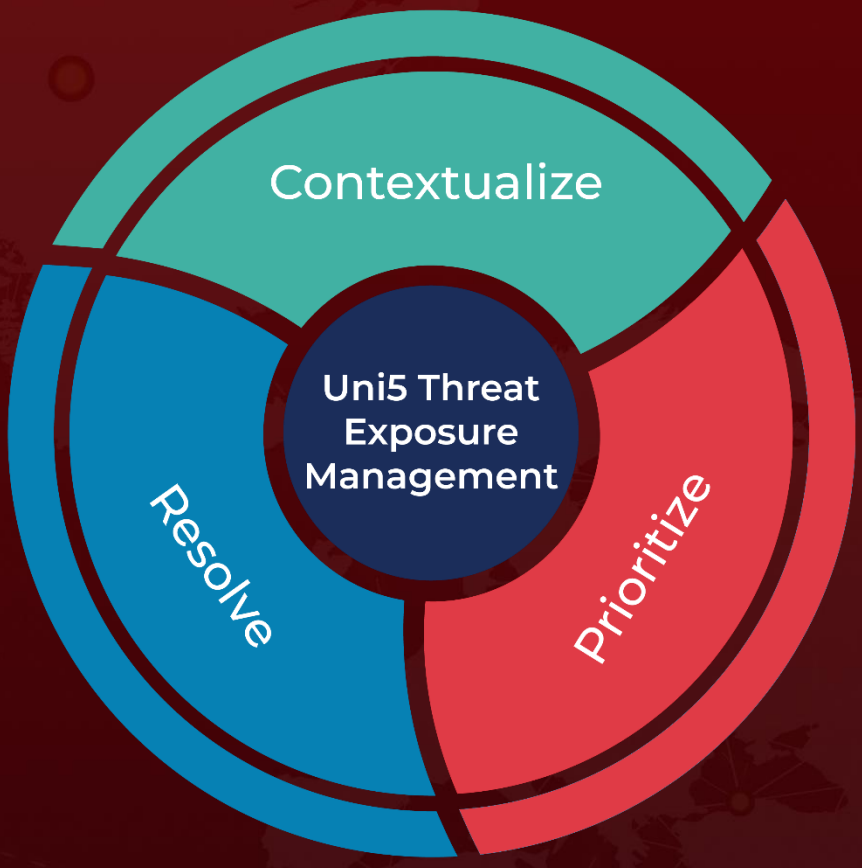
https://slcyber.io/assetnote-security-research-center/struts-devmode-in-2025-critical-pre-auth-vulnerabilities-in-adobe-experience-manager-forms/

https://www.all-about-security.de/adobe-schliesst-kritische-zero-day-luecken-in-aem-forms-nach-veroeffentlichung-von-exploit-details/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 6, 2025 . 9:30 PM

More at www.hivepro.com