Critical Adobe AEM CVEs Fixed in 2025

Business Risk Summary

MAXIMUM SEVERITY - Actively Exploited

CVE-2025-54253 (CVSS: 10.0/10 - Critical)

- Vulnerability: Unauthenticated Remote Code Execution (RCE)
- Root Cause: Misconfiguration in AEM Struts2 DevMode - exposed /adminui/debug servlet
- Affected Versions: AEM Forms on JEE versions 6.5.23.0 and earlier
- Patched: August 2025 (version 6.5.0-0108)
- **Status: Added to CISA KEV Catalog (October 15, 2025) - Actively exploited in the wild**

Business Risk:

- Allows complete system takeover without authentication
- Attackers can execute arbitrary commands remotely
- Full access to sensitive customer data, content, and business processes
- Potential for ransomware deployment, data exfiltration, or lateral movement

---

CVE-2025-54254 (CVSS: 8.6/10 - High)

- Vulnerability: XML External Entity (XXE) Injection
- Attack Vector: No user interaction required
- Affected Versions: AEM Forms on JEE versions 6.5.23.0 and earlier
- Patched: August 2025 (version 6.5.0-0108)
- **Status: Added to CISA KEV Catalog - Actively exploited**

Business Risk:

- Arbitrary file read capabilities
- Access to configuration files, credentials, and sensitive data
- Potential for Server-Side Request Forgery (SSRF)
- Data breach and compliance violations (GDPR, CCPA, etc.)

HIGH SEVERITY

CVE-2025-46982 (CVSS: 7.5/10 - High)

- Vulnerability: Stored Cross-Site Scripting (XSS)
- Affected Versions: AEM versions 6.5.22 and earlier, Cloud Service up to 2025.5.0
- Disclosed: June 10, 2025
- Patched: June 2025 (AEM Cloud Service Release 2025.9, AEM 6.5 LTS SP1)

Business Risk:

- Persistent malicious script injection
- Session hijacking and credential theft
- Compromise of user accounts and administrative access
- Defacement and brand reputation damage

CVE-2025-46981 (CVSS: 7.1/10 - High)

- Vulnerability: Stored Cross-Site Scripting (XSS)
- Attack Requirement: Low-privileged attacker access

- Affected Versions: AEM versions 6.5.22 and earlier
- Patched: Security Bulletin APSB25-90 (September 9, 2025)

Business Risk:

- Injection of malicious scripts into form fields
- Potential privilege escalation
- User data compromise and phishing attacks
- Supply chain attack vector through content distribution

Critical Business Impacts Summary

Immediate Risks:

1. Data Breach: Unauthorized access to customer PII, business-critical content, and intellectual property
2. Regulatory Compliance: GDPR, CCPA, HIPAA violations leading to significant fines
3. Business Continuity: Service disruption, ransomware attacks, system unavailability
4. Reputational Damage: Loss of customer trust, brand damage, negative media coverage
5. Financial Impact: Incident response costs, legal fees, customer compensation, lost revenue

Important Note

The fact that these vulnerabilities were added to CISA's Known Exploited Vulnerabilities catalog indicates they are being actively targeted by threat actors. Organizations running unpatched AEM instances face imminent and severe business risk.

Report Generated: November 27, 2025