CVE-2025-0133

Scor/Severitate	6.9 (MEDIU)
CWE-ID	**CWE-79** – Improper *Neutralization* of *Input During Web Page Generation* ('Cross-site Scripting')
Sisteme afectate	• Această vulnerabilitate afectează versiunile *PAN-OS* cu funcționalitățile GlobalProtect Gateway sau Portal activate. • PAN-OS 11.2: versiuni < 11.2.7 • PAN-OS 11.1: versiuni < 11.1.11 • PAN-OS 10.2: versiuni < 10.2.17 • PAN-OS 10.1: toate versiunile • Cloud NGFW: toate versiunile • Prisma Access: neafectat
Descriere	CVE-2025-0133 este o vulnerabilitate de tip *Cross-Site Scripting* (XSS) reflectat identificată în funcționalitățile *GlobalProtect Gateway* și *Portal* ale software-ului *PAN-OS* de la *Palo Alto Networks*. Această vulnerabilitate permite executarea de cod *JavaScript* malițios în contextul browserului unui utilizator autentificat în *Captive Portal*, atunci când acesta accesează un link special conceput. Principalul risc asociat este reprezentat de atacurile de tip phishing, care pot conduce la furtul de credențiale, în special dacă este activată funcționalitatea *Clientless VPN*.
Context operațional și risc extins	• Scenariu de risc sporit: Dacă organizația folosește *Captive Portal* pentru autentificarea utilizatorilor în rețele *Wi-Fi* sau de oaspeți, această vulnerabilitate poate fi ușor exploatabilă în scenarii reale, mai ales prin campanii de phishing direcționat. • Risc pentru clienți enterprise: Activarea funcționalității *Clientless VPN* implică redirecționarea traficului prin aplicații web, ceea ce extinde suprafața de atac și oferă mai multe puncte de injectare *XSS*.
Metode de exploatare	Un atacator poate crea un link special conceput care, atunci când este accesat de un utilizator autentificat în *Captive Portal*, execută cod JavaScript malițios în contextul browserului utilizatorului. Aceasta poate duce la atacuri de tip phishing și furt de credențiale, mai ales dacă *Clientless VPN* este activat.
IOC	• *URL*-uri suspicioase cu parametri injectați, precum: „https://<portal>/global-protect/login.esp?user=...<script>alert(1)</script>” • Loguri *PAN-OS* cu comportament neobișnuit: ✓ Conexiuni *HTTP* care includ stringuri nevalidate în parametri *URL* ✓ Răspunsuri web cu cod *JS* injectat în contextul *UI*
Metode de detectare	❖ Surse de log util de analizat: • ***system.log*** pentru conexiuni Captive Portal • ***threat.log*** pentru ID-uri 510003 și 510004 • ***url-filtering.log*** pentru accesări către linkuri personalizate
Mapare la standarde de securitate	Standard / Framework: OWASP Top 10 (2021) — Referință relevantă: A03:2021 – Injection ISO/IEC 27001:2022 — A.8.24 – Protecția împotriva codului malițios MITRE ATT&CK — T1059.007 – JavaScript Execution in Browser NIST SP 800-53 rev5 — SI-10: Information Input Validation
Metode de remediere	❖ Soluție oficială

	Se recomandă actualizarea la următoarele versiuni, care vor include corectivul necesar: • PAN-OS 11.2.7: estimare lansare în iunie 2025 • PAN-OS 11.1.11: estimare lansare în iulie 2025 • PAN-OS 10.2.17: estimare lansare în august 2025 • Pentru versiunile mai vechi sau neacceptate, se recomandă actualizarea la o versiune suportată care va include corectivul. ❖ Soluții temporare (workaround) • Dezactivarea Clientless VPN: Dacă această funcționalitate nu este esențială, dezactivarea ei poate reduce riscul de exploatare. • Abonament Threat Prevention: Clienții cu acest abonament pot bloca atacurile asociate acestei vulnerabilități prin activarea ID-urilor de amenințare 510003 și 510004, introduse în versiunea de conținut Applications and Threats 8970
Referință	https://security.paloaltonetworks.com/CVE-2025-0133 https://cvepremium.circl.lu/vuln/CVE-2025-0133?utm_source=chatgpt.com https://securityonline.info/palo-alto-networks-warns-of-xss-flaw-with-poc-exploit-code/?utm_source=chatgpt.com https://it.slashdot.org/story/25/02/19/2059256/palo-alto-firewalls-under-attack-as-miscreants-chain-flaws-for-root-access?utm_source=chatgpt.com https://nvd.nist.gov/vuln/detail/CVE-2025-0133 https://www.wiz.io/vulnerability-database/cve/cve-2025-0133