CVE-2025-11241 Yoast SEO Premium	
Descriere	Pluginul Yoast SEO Premium conține o expresie regulată (regex) defectuoasă folosită pentru a elimina un atribut din conținutul postărilor; această logică poate fi abuzată pentru a injecta atribute HTML arbitrare (ex. onerror, onclick) ce pot conține JavaScript. Vulnerabilitatea permite unui utilizator cu drepturi de Contributor (sau mai mari) să creeze o postare conținând payload XSS stocat care se execută în contextul altor utilizatori (ex. editor, admin)
Versiune	Yoast SEO Premium 25.7 → 25.9
CWE	CWE-80
Vector de atac și condiții	Un cont cu rol Contributor sau mai mare poate crea conținut malițios; atacatorul pregătește un payload care introduce atribute cu evenimente JavaScript sau elemente <script> acolo unde regex-ul nu curăță corect. Victimele sunt utilizatorii care vizualizează sau editează acea postare.
CVE-2025-6388 Spirit Framework	
Descriere	Funcția *custom_actions()* din Spirit Framework nu validează corespunzător identitatea utilizatorului înainte de autentificare, permițând unui atacator neautentificat care cunoaște un nume de utilizator valid să obțină acces fără parolă la acel cont (posibil admin), conducând la deturnare completă a contului.
Versiune	Spirit Framework toate versiunile <= 1.2.14
CWE	CWE-9.8
Vector de atac și condiții	Atacatorul trebuie să cunoască sau să ghicească un nume de utilizator existent (de ex. admin) — apoi folosește endpoint-ul/funcția afectată pentru a forța autentificarea fără parolă. Exploatarea este foarte periculoasă și este raportată ca activă (mass-scanning/exploit kits observate).
Impact operațional și riscuri	• CVE-2025-11241: risc de furt de sesiune, redirecționare sau execuție de script în browser; posibil pivot intern (exfiltrare token REST API, CSRF, comenzi către WP-REST), în special pe site-uri cu mulți autori/editaori. • CVE-2025-6388: risc de takeover complet al site-ului (creare backdoor, instalare plugin malițios, escaladare laterală către alte site-uri din aceeași infrastructură), pierdere totală de control și publicare de conținut malițios. Exploatarea activă crește probabilitatea compromiterii.
Detectare	• Loguri web / access logs ✓ Se vor identifica cererile direcționate către endpoint-urile asociate pluginului *Spirit Framework* (ex.: admin-ajax.php sau rute specifice *custom_actions*) care returnează cod 200 fără a urma fluxul normal de autentificare. ✓ Se vor analiza pattern-urile POST/GET neobișnuite care conțin parametri cu nume de utilizator valid, dar fără cookie de sesiune corespunzător. • Loguri WordPress (audit) ✓ Se vor examina evenimentele de autentificare pentru conturile de administrator, în special cele care nu includ evenimentul „password provided” sau prezintă modificări suspecte ale adresei IP ori ale agentului utilizator (User-Agent). ✓ Se va monitoriza activitatea utilizatorilor cu roluri Contributor sau Author, în vederea identificării postărilor care conțin atribute precum *onerror=*, *onclick=*, *<script>* sau *javascript*: în interiorul elementelor HTML. • Indicatori specifici ✓ Se vor verifica fișierele și postările care includ atribute de tip *onerror=*, *onload=*, *onclick=* sau secvențe *javascript*: în conținutul HTML. ✓ Se vor identifica cererile POST către endpoint-urile pluginului care conțin parametri cu nume de utilizator și răspunsuri care setează cookie-uri de autentificare fără proces de login valid.

Măsuri de remediere	• Pentru CVE-2025-6388 (critică, exploatare activă): ✓ Pluginul *Spirit Framework* se va actualiza la versiunea 1.2.15 sau la o versiune ulterioară care conține corecția oficială publicată de vendor. ✓ În cazul în care actualizarea nu poate fi aplicată imediat, pluginul se va dezactiva temporar prin intermediul comenzii WP-CLI (*wp plugin deactivate spirit-framework*). ✓ Se vor verifica toate conturile cu rol de administrator pentru autentificări neautorizate, iar parolele conturilor privilegiate și token-urile API se vor reseta. ✓ Se va efectua o analiză a fișierelor PHP pentru identificarea modificărilor recente, a utilizatorilor noi cu privilegii ridicate și a eventualelor pluginuri malițioase instalate. • Pentru CVE-2025-11241 (Stored XSS – Yoast SEO Premium): ✓ Pluginul *Yoast SEO Premium* se va actualiza la versiunea corectată publicată de vendor; în caz contrar, se va dezactiva temporar până la aplicarea patch-ului. ✓ Se vor revizui postările recente create de utilizatori cu roluri Contributor sau Author, pentru identificarea și eliminarea conținutului malițios care conține atribute de tip *onerror=*, *onclick=* sau *<script>*. ✓ Se vor aplica reguli WAF pentru blocarea payload-urilor XSS stocate, inclusiv filtrarea atributelor HTML cu evenimente JavaScript.
Referință	https://securityonline.info/yoast-seo-premium-flaw-stored-xss-bug-cve-2025-11241-exposes-millions-of-wordpress-sites/ https://securityonline.info/actively-exploited-critical-flaw-cve-2025-6388-cvss-9-8-allows-authentication-bypass-in-wordpress-plugin/ https://patchstack.com/database/wordpress/plugin/spirit-framework/vulnerability/wordpress-spirit-framework-plugin-1-2-14-authentication-bypass-to-account-takeover-and-privilege-escalation-vulnerability?utm_source=chatgpt.com https://nvd.nist.gov/vuln/detail/CVE-2025-6388?utm_source=chatgpt.com https://nvd.nist.gov/vuln/detail/CVE-2025-11241?utm_source=chatgpt.com