Fortinet: Zero-Day FortiWeb, CVE-2025-52970 și CVE-2025-53951

Vulnerabilitate Zero-Day FortiWeb (crearea conturilor admin)	
Identificare	Zero-day critic în FortiWeb, fără CVE publicat.
Versiunea afectate	• FortiWeb 8.0.1 – vulnerabil • FortiWeb 8.0.2 – blocat (403), indică remediere • Toate versiunile anterioare 8.0.2 trebuie considerate potențial vulnerabile.
Mecanism Tehnic	• Exploit bazat pe: ✓ JWT/payload manipulat ✓ injecție de parametri: *profname, username, vdom, loginname* ✓ acces nefiltrat către endpoint-uri interne • Vulnerabilitatea permite acces neautentificat la WebSocket CLI și la funcții administrative.
Vectorul de atac	• Interfața de management FortiWeb (GUI sau API) trebuie să fie: ✓ expusă la Internet, ✓ sau accesibilă dintr-o zonă de rețea compromisă, ✓ sau accesibilă printr-un NAT fără ACL. • Nu este necesară autentificarea. • Nu este necesară cunoașterea unor parametri secreți.
Impact	• Creare cont administrator fără autentificare („hax0r”). • Permite compromiterea completă a WAF: ✓ alterare politici, ✓ dezactivarea protecțiilor, ✓ pivotare în rețea.
CVE-2025-52970 – FortiWeb Authentication Bypass	
Identificare	• CVE: CVE-2025-52970 • Severitate: High (CVSS ~7.7) • Tip: Authentication Bypass • Cauză: CWE-233 – Improper Handling of Parameters
Versiuni afectate	Conform advisory-urilor: ✓ 7.6.0 – 7.6.3 ✓ 7.4.0 – 7.4.7 ✓ 7.2.0 – 7.2.10 ✓ 7.0.0 – 7.0.10 Fix disponibil în 8.0.2+ și versiunile patch-uite din ramurile principale.
Mecanism Tehnic	• Manevrare incorectă parametri/cookie-uri → token implicit valid. • Atacatorul induce folosirea unei chei zero-filled / valorilor implicite. • Obtine autentificare ca orice utilizator, inclusiv admin.
Vector de atac	• Network (remote) • Necesită anumite informații nepublice despre device/user → complexitate ridicată.
	Precondiții: • Atacatorul trebuie să cunoască sau să deducă anumite informații interne, precum: ✓ formatul token-urilor, ✓ identificatori de utilizator, ✓ anumite valori interne din FortiWeb (de exemplu profilul contului). • Aceasta face vulnerabilitatea „high complexity” (AC:H)
	Metoda practică de exploatare • Atacatorul trimite cereri HTTP(S) care: ✓ manipulează parametri/cookie-uri, ✓ forțează FortiWeb să folosească valori implicite (zero-filled keys) la verificarea tokenului. • Dacă verificarea tokenului cade în fallback, sistemul consideră tokenul valid. • Atacatorul devine „user X”, unde X este un utilizator existent (inclusiv „admin”)

Fortinet: Zero-Day FortiWeb, CVE-2025-52970 și CVE-2025-53951

Impact	Autentificare completă ca admin. Posibil RCE indirect (prin modificarea configurărilor și upload de fișiere).
CVE-2025-53951 – FortiDLP Agent (Outlookproxy) – Path Traversal & LPE	
Identificare	• CVE: CVE-2025-53951 • Severitate: ✓ CNA Fortinet: 5.3 – Medium ✓ NVD: 7.8 – High • Tip: Path Traversal & Local Privilege Escalation • CWE: CWE-22 – Improper Path Restriction
Versiuni afectate	FortiDLP Agent pentru Windows: 11.5.1 11.4.2 – 11.4.6 11.3.2 – 11.3.4 11.2.0 – 11.2.3 11.1.1 – 11.1.2 11.0.1 10.5.1 10.4.0 10.3.1
Mecanism Tehnic	• Componenta Outlookproxy ascultă pe un port local. • Atacatorul trimite cereri cu cale ..\..\... → ocolește directorul permis. • Operația rulează cu privilegiile LocalService → escaladare.
Vector de atac	• Local (necesită user logat sau malware prezent).
	Precondiții: • FortiDLP Agent + plugin Outlookproxy instalate și active. • Portul local Outlookproxy ascultă pe localhost (ex.: 127.0.0.1:port_dlp). • Atacatorul poate trimite cereri către acest port (prin scripturi, malware sau proces local).
	Rezultatul Exploatării: • Escaladarea privilegiilor (LPE). • Atacatorul obține acces la fișiere și procese cu drepturi superioare. • Poate ocoli politicile DLP sau instala persistenta locală.
Impact	• Escaladare privilegii LocalService. • Acces la fișiere sensibile. • Modificare logică DLP, ocolirea controalelor.
Referințe	https://cybersecuritynews.com/fortinet-fortiweb-vulnerability/ https://cybersecuritynews.com/fortiweb-authentication-vulnerability-exploited/ https://www.redpacketsecurity.com/cve-alert-cve-2025-53951-fortinet-fortidlp/ https://fortiguard.fortinet.com/encyclopedia/ips/58806?utm_source=chatgpt.com https://fortiguard.fortinet.com/psirt/FG-IR-25-448?utm_source=chatgpt.com