



Raport consolidat eveniment cibernetic

Vulnerabilități Foxit PDF

Două vulnerabilități critice au fost descoperite în aplicațiile Foxit PDF Reader și Foxit PDF Editor. Aceste vulnerabilități permit executarea de cod la distanță (RCE) pe sistemele afectate prin fișiere PDF special create.

Informații suplimentare

CVE-2024-49576	Vulnerabilitatea apare din gestionarea necorespunzătoare a obiectelor AcroForms și a obiectelor 3D din documente PDF. Aceasta poate permite atacatorilor să provoace blocarea aplicației sau să execute cod arbitrar.
CVE-2024-47810	Similar cu CVE-2024-49576, această vulnerabilitate exploatează manipularea incorectă a obiectelor, permițând atacatorilor să ruleze cod arbitrar pe sistemele afectate.
Versiuni afectate	Foxit PDF Reader: Versiunea 2024.3.0.26795 și versiunile anterioare. Foxit PDF Editor: Versiunile 11.x până la 2024.3.
Modul de atac	• Execuție de cod arbitrar: Atacatorii pot prelua controlul complet asupra sistemului afectat. • Exploatare prin fișiere PDF malițioase: Vulnerabilitățile pot fi declanșate atunci când un utilizator deschide un fișier PDF infectat sau accesează un site compromis care utilizează plugin-ul Foxit în browser.

	• Răspândire rapidă: Exploatarea poate fi realizată fără interacțiuni suplimentare din partea utilizatorului, crescând riscul de propagare.
Metode de exploatare	• Vectorul de atac: ✓ Fișiere PDF special create: Atacatorii pot trimite fișiere PDF malițioase prin e-mail sau pot încorpora cod malițios în site-uri web compromise. ✓ Exploatarea plugin-ului browser: Atacatorii pot încărca un fișier PDF într-un browser care utilizează Foxit PDF Reader/Editor pentru deschidere. ✓ Exemplu de cerere HTTP exploatabilă: „GET /document.pdf HTTP/1.1 Host: victimexample.com User-Agent: Mozilla/5.0”
IOC	• Trafic suspect către domenii necunoscute asociate fișierelor PDF. • Comportament anormal al aplicațiilor PDF (blocări sau erori frecvente). • Crearea fișierelor temporare suspecte în directoarele de utilizator. • Activitate anormală în log-uri (cereri către fișiere PDF necunoscute).
Măsuri de remediere	• Actualizare imediată : Actualizați aplicațiile Foxit PDF Reader și Editor la versiunea 2024.4 sau o versiune mai recentă. Obțineți actualizările direct de pe site-ul oficial Foxit sau utilizați mecanismul de actualizare integrat în aplicație. • Mitigări temporare ✓ Activați modul de citire sigură (Safe Reading Mode) pentru a limita execuția scripturilor și codului activ. ✓ Dezactivați integrarea browser-ului pentru deschiderea fișierelor PDF în mod automat. ✓ Blocarea descărcărilor de fișiere necunoscute prin firewall sau filtre web.

Resurse externe



<https://cybersecuritynews.com/foxit-pdf-editor-reader-vulnerabilities/>



<https://securityonline.info/cve-2024-49576-and-cve-2024-47810-foxit-addresses-remote-code-execution-flaws/>