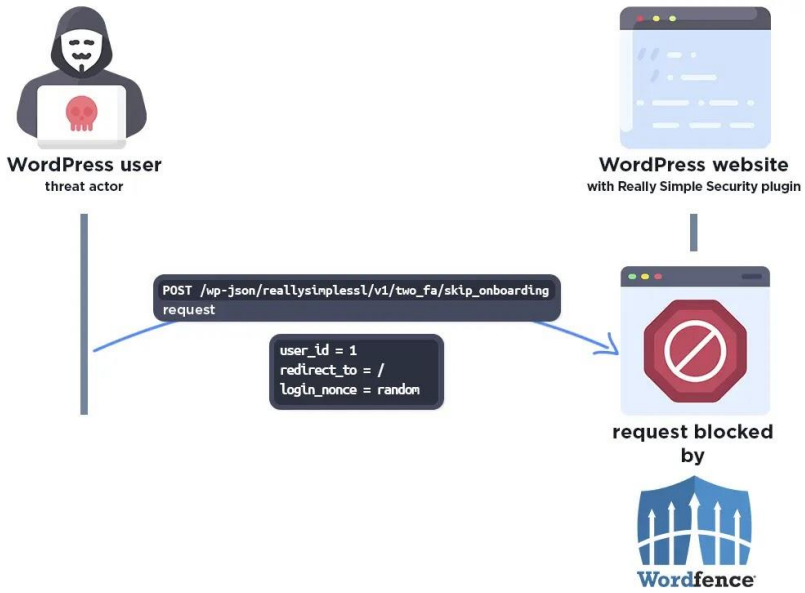
Raport consolidat eveniment cibernetic

CVE-2024-10924

O vulnerabilitate critică de tip autentificare bypass a fost descoperită în plugin-ul WordPress **Really Simple Security** (fost Really Simple SSL), utilizat de peste patru milioane de site-uri web. Vulnerabilitatea, identificată ca **CVE-2024-10924**, permite atacatorilor să obțină acces administrativ la site-uri WordPress vulnerabile fără autentificare validă.



Informații suplimentare

TIP	**Authentication Bypass**
Funcție afectată	*check_login_and_get_user()* • Această funcție verifică identitatea utilizatorilor și anume parametrii : **user_id** și **login_nonce.** • Atunci când **login_nonce** este nevalid, funcția nu respinge cererea, ci apelează **authenticate_and_redirect()**, autentificând utilizatorul pe baza exclusivă a **user_id.**
Impact	• Acces neautorizat complet la conturi, inclusiv cele cu privilegii administrative. • Vulnerabilitatea afectează site-urile care au activată autentificarea 2FA, încurajată de administratori pentru securitate suplimentară.
Versiuni afectate	• Plugin afectat: **Really Simple Security** • Versiuni vulnerabile: ***9.0.0 până la 9.1.1.1*** (toate edițiile: Free, Pro și Pro Multisite).
Metode de exploatare	❖ Vector de atac: • Atacatorii pot exploata vulnerabilitatea prin API-ul REST utilizând cereri POST manipulate. ❖ Pași pentru exploatare: • Identificarea vulnerabilității- utilizarea scanerelor automate pentru a detecta site-uri care utilizează plugin-ul vulnerabil. • Exploatarea prin *bypass* autentificare- trimiterea unei cereri *REST API* special construite pentru a autentifica un utilizator neautorizat. Exemplu de cereri REST API: „*POST /wp-json/rss/v1/authenticate HTTP/1.1* *Host: example.com* *Content-Type: application/json* *{* *"user_id": "1",* *"login_nonce": "invalid_nonce"* *}”*
IOC	• Trafic suspect către **/wp-json/rss/v1/authenticate.** • Crearea sau modificarea neașteptată a conturilor administrative. • Logări neautorizate în interfața de administrare **WordPress.** • Activitate anormală în logurile de acces și erori.

Măsuri de remediere	❖ **Actualizare imediată:** • Actualizați plugin-ul la **versiunea 9.1.2** sau mai recentă. ❖ **Mitigări temporare:** • **Dezactivarea API-ului REST pentru plugin:** • Utilizați un plugin suplimentar sau configurați serverul pentru a bloca accesul la endpoint-ul /wp-json/rss/v1/authenticate. ❖ **Restricționarea accesului la site:** • Configurați firewall-ul pentru a permite doar IP-uri de încredere să acceseze panoul de administrare. **Măsuri suplimentare:** • Configurați reguli de rate limiting pentru a limita numărul cererilor către endpoint-uri REST. • Monitorizați și analizați logurile pentru activități suspecte.
Recomandări suplimentare	❖ **Monitorizare continuă:** Utilizați un plugin de securitate pentru a monitoriza accesul API. ❖ **Implementați rate limiting:** Limitați numărul de cereri către API-ul REST. ❖ **Educație pentru administratori:** Informați utilizatorii despre riscurile 2FA incorect configurate.

Resurse externe

- https://www.bleepingcomputer.com/news/security/security-plugin-flaw-in-millions-of-wordpress-sites-gives-admin-access/
- https://cybersecuritynews.com/wordpress-plugin-vulnerability/
- https://www.wordfence.com/blog/2024/11/really-simple-security-vulnerability/