Raport consolidat eveniment cibernetic

CVE-2024-10960

Vulnerabilitatea CVE-2024-10960 este cauzată de validarea inadecvată a tipurilor de fișiere în funcția ***storeUploads***, permițând atacatorilor autentificați cu rol de *Contributor* sau superior să încarce fișiere arbitrare pe server. Acest lucru poate duce la execuție de cod la distanță (RCE - Remote Code Execution), compromițând grav securitatea site-ului afectat.

Informații suplimentare

Tip	Încărcare de fișiere arbitrare (Arbitrary File Upload).
Versiunea afectate	Până la și inclusiv 2.6.4.
Plugin afectat	Brizy - Page Builder pentru WordPress**.**
Vector de atac	Acces autenticat (Contributor sau superior).
Impact	❖ Atacatorii pot încărca și executa fișiere malițioase pe server. ❖ Se poate obține control asupra site-ului WordPress afectat. ❖ Datele și fișierele stocate pe server pot fi compromise. ❖ Există posibilitatea escaladării privilegiilor și exploatării suplimentare a infrastructurii.
Metoda de Exploatare	❖ Un utilizator autentificat cu rol de Contributor sau superior încarcă un fișier malițios (ex: un script PHP backdoor) folosind funcția ***storeUploads*** din plugin. ❖ Fișierul este plasat într-o locație accesibilă și executabilă pe server, cum ar fi ***/wp-content/uploads/***. ❖ Atacatorul identifică locația exactă a fișierului încărcat prin scanarea directoarelor accesibile folosind instrumente precum ***dirb***, ***gobuster*** sau ***wfuzz***.

	❖ Odată ce locația fișierului este cunoscută, atacatorul inițiază o cerere HTTP către fișierul PHP malițios prin browser sau prin ***curl/wget.*** ❖ Execuția scriptului PHP permite atacatorului să ruleze comenzi pe server și să escaladeze atacul, potențial obținând acces root.
Porturi și Protocoale inplicate	❖ Port 80/443 (HTTP/HTTPS): Utilizat pentru a încărca fișiere și a declanșa execuția codului malițios. ❖ Port 21 (FTP): Dacă este activ, poate fi utilizat pentru a verifica fișierele încărcate. ❖ Port 22 (SSH): Poate fi utilizat pentru escaladarea atacului dacă atacatorul reușește să obțină credențiale.
Instrumente pentru Scanare	❖ ***dirb, gobuster, wfuzz*** - pentru identificarea fișierelor încărcate. ❖ ***nmap*** - pentru detectarea serviciilor active și a versiunilor acestora. ❖ ***sqlmap*** - în cazul în care sunt descoperite vulnerabilități SQL Injection adiacente. ❖ ***Metasploit*** - pentru testarea exploatării și escaladării privilegiilor.
Soluții și Mitigare	❖ Actualizare imediată: Se recomandă actualizarea pluginului Brizy la versiunea 2.6.5 sau o versiune ulterioară, care conține un patch de securitate pentru această vulnerabilitate. ❖ Restricționarea rolurilor de utilizator: Limitarea conturilor Contributor sau superior numai la utilizatorii de încredere. ❖ Configurarea serverului: Implementarea unor reguli stricte pentru încărcarea de fișiere, inclusiv restricționarea executării scripturilor în directoare neautorizate. ❖ Monitorizare și audit: Verificarea logurilor pentru activități suspecte legate de încărcarea fișierelor și implementarea unor soluții de detecție a amenințărilor.