UPDRAFTPLUS · UPDRAFTCENTRAL · WORDPRESS · SECURITATE

Cineva are cheia site-ului tău? Verifică azi.

Ghid pas cu pas după breșa UpdraftPlus din octombrie 2026: cum afli dacă site-ul e afectat, unde se ascunde backdoor-ul și cum îl cureți fără să strici nimic.



+ Ce s-a întâmplat
+ Ești afectat?
+ Semnele backdoor-ului
+ Cei 7 pași
+ Comenzi WP-CLI
+ Checklist lunar

01 · CE S-A ÎNTÂMPLAT

Nu un bug. O cheie furată.

UpdraftPlus are peste 4 milioane de instalări active pe WordPress.org. Firma care îl face, TeamUpdraft, oferă și UpdraftCentral: un panou din care agențiile administrează mai multe site-uri. Cheile acestui panou au ajuns la atacatori.

DATA (2026)	CE S-A ÎNTÂMPLAT	SURSA
17–18 octombrie	Acces neautorizat pe teamupdraft.com. E accesată baza de date cu clienții, inclusiv cheile UpdraftCentral.	TeamUpdraft
18 oct., după-amiază	**Primele pluginuri ascunse instalate pe site-uri conectate**	Patchstack
19 oct., dimineață	Ultima instalare văzută de Patchstack. Nethemba descoperă atacul pe 3 site-uri proprii.	Patchstack
19 octombrie	UpdraftPlus 1.26.12, apoi 1.26.13 (Premium 2.26.13): revocă cheile vechi	WordPress.org
29 octombrie	**Confirmare: pe unele site-uri s-au creat conturi de administrator chiar după deconectare**	TeamUpdraft

CE A FOST EXPUS

Datele contului TeamUpdraft

- Nume, email, adresă de facturare, istoric comenzi
- Parole criptate, setări de autentificare în doi pași
- **Cheile UpdraftCentral, UpdraftVault și UpdraftClone**

CE NU A FOST ATINS

Pluginul și backup-urile tale

- Pluginul UpdraftPlus de pe WordPress.org
- Backup-urile din Google Drive, Dropbox, S3 etc.
- UpdraftCentral instalat pe serverul tău; datele de card (Stripe, PayPal)

DE CE CONTEAZĂ: o cheie validă trece de orice verificare. Site-ul a executat comenzile atacatorului ca și cum ar fi venit de la panoul legitim.

02 · EȘTI AFECTAT?

Patru situații. Una e a ta.

Riscul depinde de un singur lucru: dacă site-ul a fost conectat vreodată la UpdraftCentral, în cloud. Dacă de site se ocupă o agenție sau un freelancer, e posibil să fi fost conectat fără să știi.

SITUAȚIA TA	RISC	CE FACI
Site-ul a fost conectat la UpdraftCentral (de tine sau de agenție)	**Mare**	Toți cei 7 pași (paginile 04–05)
Ai cont pe teamupdraft.com (Premium, UpdraftVault, UpdraftClone)	Mediu	Parolă nouă, reset la autentificarea în doi pași, apoi verifici site-urile
Doar UpdraftPlus gratuit, fără cont, fără UpdraftCentral	Mic	Actualizezi pluginul și verifici cheile (pasul 2)
Site pe Shopify, Gomag sau altă platformă închiriată	Fără legătură	Nimic

ÎNTREABĂ AGENȚIA copiază mesajul

„Bună ziua. După incidentul TeamUpdraft din 17–18 octombrie 2026: site-ul nostru a fost conectat vreodată la UpdraftCentral? Dacă da, ați șters cheile, ați verificat pluginurile (inclusiv mu-plugins) și utilizatorii și ați schimbat cheile de securitate WordPress? Vă rog să ne trimiteți și lista serviciilor externe care au acces la site.”

NU ȘTII SIGUR? Patchstack recomandă verificarea și dacă ești convins că nu ai folosit UpdraftCentral: opțiunea de conectare e bifată din start. Pasul 2 îți arată în 1 minut dacă există o cheie pe site.

03 · SEMNELE BACKDOOR-ULUI

Ce cauți. Exact.

Backdoor-ul e un plugin care așteaptă un cod secret de 32 de caractere. Când îl primește, creează un cont și îl loghează pe atacator direct, prin cookie, fără formularul de login și fără autentificarea în doi pași. Contul rămâne și după ce ștergi pluginul.

SEMN	CUM ARATĂ	UNDE ÎL VEZI
PLUGINUL ASCUNS		
Descrierea	**„Small maintenance toolkit: keeps option storage tidy."**	Module → Module instalate sau fișierul principal al pluginului. Cel mai sigur semn, după Patchstack.
Numele	99 de variante: Site Health Cache, Asset Forge 2, Speed Kit, Seo Helper, Content Helper, Query Shelf, Nav Hub, Link Latch…	`wp-content/plugins` și `wp-content/mu-plugins`
CONTUL CREAT		
Nume afișat	**„Site Tools"**	Utilizatori → toți utilizatorii
Utilizator	două cuvinte + cifre: data-ops43, media-staff96, web.tech988, cms.tech644	Rolul afișat e Editor, dar are drept de setări și de instalare pluginuri
Email	o adresă @example.org	Coloana Email din lista de utilizatori
Baza de date	o opțiune al cărei nume se termină în `_sync_token`	Tabelul `wp_options` (phpMyAdmin)
ÎN LOGURI		
IP-uri	43.250.53.42 și 2a09:bac5:4e21:2e3c::49b:9	Logurile de acces ale hostingului. Atacatorul a schimbat infrastructura, deci lipsa lor nu dovedește nimic.

NU REPARA eroarea 500 e un semn, nu o problemă de rezolvat

> Primele variante ale backdoor-ului aveau o greșeală de cod și blocau site-ul cu eroarea 500. Dacă cineva „repară" pluginul, backdoor-ul începe să funcționeze. Un plugin necunoscut care dă eroare se dezactivează și se mută, nu se repară.

04 · PAȘII 1-3, DIN PANOU

Primii trei pași îi faci singur.

După avizul TeamUpdraft și recomandările Patchstack. Ai nevoie de contul de administrator WordPress și de acces la managerul de fișiere al hostingului (cPanel, Plesk sau panoul firmei tale).

01

Actualizează UpdraftPlus

La **1.26.13** sau mai nou (Premium: **2.26.13**). Pe 26 octombrie WordPress.org avea 1.26.14. Actualizarea deconectează legăturile cu UpdraftCentral făcute înainte de 18 octombrie, ora 13:07 (ora Londrei). Versiunea 1.26.12 avea o greșeală și nu ștergea cheile corect.

02

Șterge toate cheile UpdraftCentral

Setări → UpdraftPlus Backups → Advanced Tools → UpdraftCentral → Manage existing keys și șterge-le pe toate. Cheile nu expiră. Dacă ștergi site-ul doar din panoul UpdraftCentral, cheia rămâne activă pe site.

03

Verifică pluginurile, și pe cele ascunse

În managerul de fișiere deschide **wp-content/plugins** și **wp-content/mu-plugins**. Pluginurile din mu-plugins pornesc automat și nu apar în lista obișnuită. Orice folder pe care nu-l recunoști e suspect. Dezactivează-l, apoi mută sau șterge folderul direct din fișiere, nu din panoul WordPress.

- [ ] Notează numele și data fiecărui folder suspect înainte să-l muți. Îți trebuie dacă ceri ajutor.
- [ ] Compară cu lista pluginurilor pe care le știi. Un plugin cu un nume generic, instalat pe 18 sau 19 octombrie, e aproape sigur backdoor-ul.
- [ ] Fă un backup al site-ului în starea actuală înainte de orice ștergere, separat de backup-urile vechi.

05 · PAȘII 4-7

Conturi, sesiuni, parole noi.

04 Verifică utilizatorii

Toți administratorii și editorii. Caută „Site Tools”, emailuri @example.org și conturi create pe 18–19 octombrie sau după. Șterge contul atacatorului și opțiunea `_sync_token`.

05 Închide toate sesiunile

Schimbă cheile de securitate WordPress (salts) din `wp-config.php`. Toată lumea e delogată, inclusiv atacatorul. Apoi schimbă parolele administratorilor și editorilor reali și pornește autentificarea în doi pași.

06 Restaurează, dacă ai găsit ceva

Dintr-un backup făcut **înainte de 17 octombrie**, după ce verifici că nu conține pluginul suspect. Detalii la pagina 06.

07 Reconectează la final

UpdraftCentral doar după toate verificările. Patchstack recomandă să aștepți explicația completă a TeamUpdraft. UpdraftVault cere reconectare oricum.

PENTRU DEVELOPER WP-CLI, comenzile din avizul TeamUpdraft și Patchstack

```
# există o cheie UpdraftCentral? orice rezultat = site expus
wp option get updraft_central_localkeys

# șterge toate cheile
wp option delete updraft_central_localkeys

# administratori și editori, fără să încarci pluginurile (și backdoor-ul)
wp user list --role=administrator --skip-plugins
wp user list --role=editor --skip-plugins

# chei de securitate noi: toate sesiunile se închid
wp config shuffle-salts
```

06 · DACĂ AI GĂSIT BACKDOOR-UL

Backup-ul vechi e acum aur.

Dacă ai găsit contul „Site Tools", pluginul cu descrierea de la pagina 03 sau codul secret în loguri, Patchstack spune să tratezi site-ul ca fiind complet compromis. Atacatorul a avut drepturi de administrator, deci putea lăsa și alte surprize.



A

Alege backup-ul

Ultimul făcut înainte de 17 octombrie 2026. Dacă ții backup-uri doar 7 zile, s-ar putea să nu-l mai ai: întreabă și firma de hosting, multe păstrează copii proprii.

B

Restaurează și compară

Compară fișierele WordPress cu o instalare curată (`wp core verify-checksums`) și verifică din nou pluginurile și utilizatorii.

C

Schimbă tot

Parolele de administrator, parola contului TeamUpdraft, datele de acces la stocarea backup-urilor (Google Drive, Dropbox, S3), autentificarea în doi pași.

D

Ai magazin? Verifică comenzile

Pagina de plată, adresele de plată, emailurile automate. Un administrator poate schimba oricare dintre ele.

07 · UNELTE RECOMANDATE

Ca să vezi data viitoare.

Backdoor-ul din octombrie nu se vedea din exterior. Cu un jurnal de activitate ai fi văzut pe loc pluginul instalat și contul nou. Toate uneltele de mai jos au variantă gratuită, mai puțin Patchstack.

UNEALTĂ	CE FACE	CE TREBUIE SĂ ȘTII
JURNAL DE ACTIVITATE		
WP Activity Log wordpress.org/plugins/wp-security-audit-log	Înregistrează cine a instalat un plugin, cine a creat un utilizator și când.	Peste 300.000 de instalări, notă 4,7. Făcut de Melapress.
SCANARE ȘI FIREWALL		
Wordfence Security wordpress.org/plugins/wordfence	Scanează fișierele după malware și compară cu WordPress original. Firewall și autentificare în doi pași.	Peste 5 milioane de instalări, notă 4,7. În varianta gratuită, regulile noi vin cu 30 de zile întârziere.
Patchstack patchstack.com	Alerte de vulnerabilități și reguli care blochează atacuri înainte să existe un update.	Serviciu plătit, cu perioadă de probă. Firma care a analizat atacul din octombrie.
AUTENTIFICARE ÎN DOI PAȘI		
Two Factor wordpress.org/plugins/two-factor	Cod din aplicație (Google Authenticator, Authy), cod pe email, coduri de rezervă.	Plugin oficial WordPress.org, peste 100.000 de instalări, notă 4,7.
BACKUP		
UpdraftPlus wordpress.org/plugins/updraftplus	Backup programat în Google Drive, Dropbox sau S3. Rămâne o alegere bună.	Problema a fost conexiunea UpdraftCentral, nu backup-ul. Ține backup-urile cel puțin 30 de zile.

ATENȚIE: autentificarea în doi pași nu ar fi oprit acest atac (backdoor-ul ocolește login-ul), dar oprește cele mai multe atacuri cu parole furate.

TRANSPARENȚĂ: nu suntem afiliați cu aceste produse. Paginile au fost verificate pe 2 noiembrie 2026.

08 · CHECKLIST LUNAR

30 de minute pe lună.

Breșa UpdraftPlus a venit după PHP2Shell (21 octombrie) și, după Patchstack, e al doilea incident pe canalul UpdraftCentral în cinci luni. Un site WordPress cere verificare lunară. Asta facem în mentenanță pentru clienții noștri.

ÎN FIECARE LUNĂ

bifează și notează data

- [ ] **Actualizări:** WordPress, temă, pluginuri și versiunea PHP de la hosting.
- [ ] **Utilizatori:** lista administratorilor și editorilor. Șterge conturile foștilor angajați și ale agențiilor cu care nu mai lucrezi.
- [ ] **Pluginuri:** inclusiv folderul mu-plugins. Dezinstalează ce nu mai folosești.
- [ ] **Conexiuni externe:** UpdraftCentral, ManageWP, MainWP, Jetpack, parole de aplicație. Fiecare e o ușă în plus.
- [ ] **Backup:** există, e în afara hostingului, are cel puțin 30 de zile și ai făcut o restaurare de probă.
- [ ] **Jurnalul de activitate:** instalări de pluginuri și conturi noi pe care nu le recunoști.
- [ ] **Search Console:** secțiunea Probleme de securitate și paginile noi indexate pe care nu le-ai creat.

O DATĂ PE AN

sau când schimbi agenția

> Schimbă parolele de administrator, cheile de securitate WordPress și parolele de la hosting și de la stocarea backup-urilor. Cere în scris lista serviciilor externe conectate la site și cine are acces la ele.

09 · PLATFORMA

Cine se ocupă de securitate?

Pe Shopify, serverele și actualizările sunt treaba platformei. Pe WooCommerce și pe un magazin custom, sunt treaba ta sau a echipei tale. Facem toate trei și îți spunem sincer ce se potrivește.

SECURITATEA E A PLATFORMEI

Shopify

Fără pluginuri de backup de instalat și fără PHP de actualizat. Aplicațiile din Shopify App Store cer permisiuni explicite, pe care le poți revoca oricând.

- **Mentenanță tehnică:** făcută de Shopify
- **Magazin de la:** aproximativ 500 EUR

Cere ofertă pentru un magazin Shopify →

CONTROL TOTAL

WooCommerce

Codul și datele sunt ale tale, iar securitatea e o muncă lunară. O includem în mentenanță: actualizări, backup în afara hostingului, jurnal de activitate, verificarea utilizatorilor.

- **Unelte:** UpdraftPlus, WP Activity Log, Wordfence, Two Factor

Cere ofertă pentru un magazin WooCommerce →

CONSTRUIT LA COMANDĂ

Custom

Magazin sau site construit de la zero, fără pluginuri de la terți, cu acces la distanță doar unde îl vrei tu.

Cere ofertă pentru un magazin custom →

PE SCURT

Șterge cheile.
Verifică azi.

Facem site-uri și magazine Shopify, WooCommerce și custom pentru afaceri din România. Dacă ai deja un site WordPress, facem verificarea completă pentru breșa UpdraftPlus și ne ocupăm lunar de actualizări, backup-uri și utilizatori, în pachetul de mentenanță.

VEZI PACHETELE DE MENTENANȚĂ

Ofertă: elevateweb.ro/contact · Shopify: elevateweb.ro/shopify · WooCommerce și custom: elevateweb.ro/magazin_online

Articolul complet, cu sursele: elevateweb.ro/blog/updraftplus-bresa-securitate

Surse: teamupdraft.com (aviz din 19 octombrie 2026, actualizat pe 29 octombrie), patchstack.com (19 octombrie 2026), WordPress.org, BleepingComputer (20 octombrie 2026), The Hacker News (21 octombrie 2026). Verificat pe 2 noiembrie 2026.