

TeamUpdraft breach: stolen UpdraftCentral keys used to backdoor WordPress sites



TeamUpdraft reported unauthorised access to its website on 17-18 October. Attackers are reportedly using stolen UpdraftCentral keys to install backdoor plugins and create administrator accounts on connected WordPress sites.

- TeamUpdraft detected unauthorised access over the weekend of 17-18 October and believes its customer database was accessed.
- The data included password hashes, two-factor settings and connection keys for UpdraftCentral, UpdraftVault and UpdraftClone.
- Patchstack says attacks began on 18 October at 15:32 UTC, running code and adding full administrator accounts; at least 99 differently named malicious plugins were logged.
- An estimated 10% of UpdraftPlus sites hold an UpdraftCentral or Migrator key, potentially around

400,000 websites.

- Users should update UpdraftPlus to 1.26.13 (free) or 2.26.13 (Premium) or later and delete existing UpdraftCentral keys.

TeamUpdraft, the developer of the UpdraftPlus backup plugin and related WordPress tools, said it found unauthorised access to its website over the weekend of 17-18 October. It closed the access route, signed out all accounts and replaced keys and credentials that may have been affected.

What was exposed

The vendor believes the attacker reached its customer database. This held customer and billing details, order history, password hashes, two-factor authentication settings and connection keys for UpdraftCentral, UpdraftVault and UpdraftClone. TeamUpdraft says it stores no payment details, that UpdraftPlus plugin files and downloads are unaffected, and that self-hosted UpdraftCentral instances are not impacted.

Active exploitation

Patchstack reports that attackers are using stolen keys against sites connected to UpdraftCentral, with activity starting on 18 October. The attacks run arbitrary code and add administrator accounts. At least 99 malicious plugins were logged, disguised as maintenance or optimisation tools. Nethemba documented attacks on three of its own sites, two of which received a malicious plugin, and noted the commands were signed with valid keys rather than exploiting a flaw. It also reports that the vendor's first fix release, 1.26.12/2.26.12, failed to remove the cloud keys because of a bug.

An estimated 10% of UpdraftPlus sites have an UpdraftCentral or Migrator key, which could expose around 400,000 websites.

Organisations that manage WordPress sites through UpdraftCentral should treat the keys as compromised and act without waiting for signs of intrusion.

What to do now

1. Identify all WordPress sites, including those run by agencies or vendors, that use UpdraftPlus or UpdraftCentral.
2. Update UpdraftPlus to 1.26.13 (free) or 2.26.13 (Premium) or later, then delete existing UpdraftCentral connection keys in each site's settings.
3. Rotate storage credentials and reauthorise connections for sites that were accessed through UpdraftCentral.
4. Review logs and files for indicators published by TeamUpdraft, Patchstack and Nethemba, and check for unknown plugins and new administrator accounts.

5. If compromise is confirmed, restore from clean backups, change the TeamUpdraft account password, revoke all sessions and reset the two-factor method.
6. Assess whether personal data on affected sites triggers incident handling and notification duties under your internal procedures and PDPL.