TeamUpdraft Breach Exposes UpdraftCentral Keys Used to Backdoor WordPress Sites

Unknown attackers breached TeamUpdraft's website and may have accessed customer connection keys for UpdraftCentral, UpdraftVault and UpdraftClone, then used them to plant backdoors on WordPress sites.

- Unknown actors breached the website of TeamUpdraft, the developer of the UpdraftPlus backup plugin.
- Customer connection keys for UpdraftCentral, UpdraftVault and UpdraftClone were potentially accessed.
- The keys were reportedly used to backdoor WordPress sites.
- UpdraftPlus has more than four million active installations, so the potential exposure is broad.
- The source excerpt does not give details on the backdoor or on the number of affected sites.

Unknown threat actors have breached the website of TeamUpdraft, the vendor behind UpdraftPlus, a widely used WordPress backup plugin with more than four million active installations. According to the report, the attackers may have obtained customers' connection keys for UpdraftCentral, UpdraftVault and UpdraftClone, and used them to place backdoors on WordPress sites.

Why it matters

Connection keys act as credentials that link a site to remote management and backup services. If a key is exposed, an attacker may be able to act through that trusted channel without needing the site's own login. For organisations that rely on UpdraftPlus or its companion services, the concern is both a possible compromise of the website and of the backups tied to it.

The source excerpt is limited. It does not describe how the backdoors work, how many sites were affected, or what remediation TeamUpdraft has issued. Readers should check the vendor's official communications for those details rather than assume them.

What to do next

Organisations running WordPress should first establish whether they use UpdraftPlus, UpdraftCentral,

UpdraftVault or UpdraftClone, including on sites managed by agencies or third parties. Where they do, treat the connection keys as potentially exposed and review the sites for unexpected changes. Handling should follow the institution's incident response and third-party risk processes.

What to do now

1. Inventory all WordPress sites, including those run by agencies, and identify any using UpdraftPlus, UpdraftCentral, UpdraftVault or UpdraftClone.
2. Revoke and regenerate UpdraftCentral, UpdraftVault and UpdraftClone connection keys for affected sites.
3. Review sites for unexpected admin users, modified or unfamiliar files and unusual plugin or theme changes.
4. Check the integrity and access logs of backups stored through UpdraftVault or linked services.
5. Monitor TeamUpdraft's official advisories and apply any fixes or guidance it publishes.
6. Open an incident record and inform third-party risk owners if a compromise is suspected.