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 backdoor WordPress sites.

- Unknown threat actors breached the website of TeamUpdraft, the developer of UpdraftPlus.
- Customer connection keys for UpdraftCentral, UpdraftVault and UpdraftClone were potentially accessed.
- The keys were reportedly used to plant backdoors on WordPress sites.
- UpdraftPlus is a widely used backup plugin with over four million active installations.

What happened

Unknown threat actors breached the website of TeamUpdraft, the company behind the UpdraftPlus WordPress backup plugin. The attackers potentially gained unauthorized access to customers' connection keys for UpdraftCentral, UpdraftVault and UpdraftClone, and used them to backdoor WordPress sites.

UpdraftPlus has more than four million active installations. TeamUpdraft also offers UpdraftCentral, a remote management product for WordPress sites. The source excerpt does not give further detail on the scope of the compromise, the number of affected sites or the technical method of the backdoors.

Why it matters

Connection keys act as trusted credentials between a site and the management or storage service. If such keys are exposed, an attacker may be able to act on a site without exploiting any flaw in it. Organizations that use these products for corporate or public-facing WordPress sites should treat the keys as potentially compromised until the vendor's guidance says otherwise.

What to do next

Check whether your organization, or any agency or contractor managing your web properties, uses UpdraftPlus, UpdraftCentral, UpdraftVault or UpdraftClone. If so, review the vendor's official notice, rotate the connection keys and look for signs of unauthorized changes on the affected sites.

What to do now

1. Inventory all WordPress sites, including those run by agencies or contractors, that use UpdraftPlus, UpdraftCentral, UpdraftVault or UpdraftClone.
2. Rotate or regenerate the connection keys for these products and revoke old ones.
3. Review the vendor's official advisory and follow its remediation steps.
4. Scan affected sites for unknown admin users, modified files, unfamiliar plugins and other signs of backdoors.
5. Review backup storage and remote management access logs for unexpected activity.
6. Report confirmed incidents to your security team and, where required, to the relevant authority under your incident-reporting obligations.