

FOR IMMEDIATE RELEASE

October 22, 2026

Limehawk Urges WordPress Site Owners Using UpdraftPlus to Update After Vendor Breach

TeamUpdraft says an attacker used UpdraftCentral connections to customer sites to create admin accounts and install malicious plugins. The update revokes those keys; sites still need checking.

KNOXVILLE, Tenn., Oct. 22, 2026. Limehawk, LLC, a Knoxville managed IT services provider, today urged WordPress site owners who use the UpdraftPlus backup plugin to confirm they are on version 1.26.13 (free) or 2.26.13 (Premium) and to check their sites for signs of tampering, after a security incident at the plugin's maker, TeamUpdraft.

TeamUpdraft says that "over the weekend of 17-18 October we identified unauthorised access to the teamupdraft.com website" and that "we believe our customer database was accessed." According to TeamUpdraft, that database holds names, email and billing addresses, order history, hashed account passwords, two-factor authentication settings, and connection keys for UpdraftCentral, UpdraftVault and UpdraftClone. TeamUpdraft says it does not store card details.

TeamUpdraft also says: "The attacker exploited the connection to users' sites to create admin accounts, install malicious plugins etc." It adds that the extent of that is unknown.

TeamUpdraft says the UpdraftPlus 1.26.13 and 2.26.13 update, released Oct. 19, "automatically disconnects user sites from UpdraftCentral by revoking connection keys," and that WordPress.org pushed it to all users. It also says "it's still important that users check over their sites for suspicious activities." According to TeamUpdraft, the UpdraftPlus plugin and its downloads were not affected, and neither were backups in your own remote storage or self-hosted UpdraftCentral.

Why does this matter for businesses?

Small business WordPress sites can rely on backup plugins like UpdraftPlus, and an unknown admin account or plugin can give an attacker control of the site.

What should site owners do?

Limehawk recommends these steps:

- **Confirm the version.** Log in to each site's own WordPress dashboard and check that UpdraftPlus is 1.26.13 (free) or 2.26.13 (Premium) or later.

- **Check users.** TeamUpdraft says to look for any users you don't recognize, not only administrators, and remove them, and that "we're seeing a pattern of unexpected 'editor' roles especially."
- **Check plugins.** Look under Plugins, including the Must-Use tab if you can see it, and remove anything you don't recognize.
- **Check logs.** TeamUpdraft lists "IPs you don't recognise in the logs" as a warning sign.
- **Change passwords.** Change every administrator password on the site, and your teamupdraft.com password if you have an account.
- **Check Premium sites too.** TeamUpdraft says UpdraftPlus Premium users should check "even if you've never used UpdraftCentral."
- **Review UpdraftCentral.** TeamUpdraft says to log in via My Account and look at the sites listed: "Any site listed before this incident has potentially been exposed to the attacker."

What if a site was tampered with?

TeamUpdraft says to consider restoring the site from a backup taken before Oct. 17. If a site was accessed through UpdraftCentral, it also says to re-authorize remote storage and change any storage access keys as a precaution.

Sources

1. TeamUpdraft, "TeamUpdraft security incident: What customers need to know." Last updated Oct. 22, 2026.
<https://teamupdraft.com/blog/security-incident-october-2026/>
2. WordPress.org, "UpdraftPlus: WP Backup & Migration Plugin." Changelog for version 1.26.13, Oct. 19, 2026.
<https://wordpress.org/plugins/updraftplus/>

Media Contact

Corey Watson, Managing Member
Limehawk, LLC
press@limehawk.io
<https://limehawk.io>

###