

UpdraftPlus WordPress Plugin Security Breach Enables Backdoor Attacks via @sejournal, @martinibuster

A security breach affecting UpdraftPlus, a WordPress backup plugin installed on over 3 million websites, enabled attackers to install malicious plugins and create unauthorized administrator accounts. The attack exploited compromised UpdraftCentral connection keys, allowing attackers to take control of connected WordPress websites without needing a username or password.

Updraft Website Compromised

TeamUpdraft confirmed that its website was compromised over the weekend of October 17-18, 2026. The company believes attackers accessed its customer database, which contained customer information and connection keys for services including UpdraftCentral. Those compromised keys enabled attackers to gain control of connected WordPress websites.

Updraft Security Response

A TeamUpdraft blog post explained that the unauthorized access route at the heart of the breach was closed, that the potentially compromised credentials were replaced, and that security updates were released that revoke older UpdraftCentral connections.

The updates, UpdraftPlus 1.26.13 for the free version and

2.26.13 for the premium version, were released on October 19, 2026.

The plugin changelog describes the updates as revoking UpdraftCentral Cloud keys, with version 1.26.13 correcting how the revocation was applied in the preceding release. The updates automatically disconnect affected websites from UpdraftCentral, blocking further access through that route.

The company also reported that WordPress.org had pushed the updated plugin to users automatically.

UpdraftPlus WordPress Backup Plugin

The UpdraftPlus plugin is used by WordPress websites to create backups, restore websites, and migrate sites to different hosting providers or domain names. It supports automated backups and enables website owners to store backup copies of their websites on services such as Google Drive, Dropbox, and Amazon S3.

The plugin also includes UpdraftCentral, a remote management feature that enables website owners to manage multiple WordPress installations from a single dashboard. That feature is at the center of the security incident.

The Compromise Of UpdraftCentral

UpdraftCentral uses security keys to authenticate instructions sent from the remote dashboard to connected websites. Those keys allow the service to perform administrative actions without requiring someone to log in to each website separately.

Compromised Security Keys Enable Website

Takeover

The compromised UpdraftCentral keys enabled attackers to send commands to connected WordPress websites that appeared to be legitimate instructions from the remote management service.

Standard security checks couldn't distinguish between legitimate instructions and those authenticated with stolen keys. As a result, WordPress websites accepted the attackers' commands as authorized.

In security company Patchstack's initial analysis, published before TeamUpdraft released the security updates, the issue was explained as not an actual vulnerability:

"This is not a vulnerability in UpdraftPlus, and as of 19 October no plugin update stops it. The commands are correctly encrypted and signed with genuine dashboard private keys. Every check in the plugin passes, because from the site's point of view the instruction is legitimate."

What that means is that the attackers weren't exploiting a programming error in the UpdraftPlus plugin itself. The security checks were working as designed, but the stolen keys allowed attackers to impersonate the remote management service.

Malicious Plugins Installed

Using the compromised UpdraftCentral security keys, attackers sent commands to connected WordPress websites instructing them to install and activate malicious plugins. Because the commands were authenticated with genuine security keys, the websites treated them as legitimate instructions and installed the plugins through WordPress's normal plugin installation process.

The malicious plugins contained a backdoor that could create a

WordPress user account with the Editor role and then grant that account additional administrative permissions.

Although an Editor account normally lacks permission to install plugins or manage important WordPress settings, the malicious code separately granted those capabilities. That made the unauthorized accounts difficult to identify because they could appear to be ordinary Editors while possessing permissions normally reserved for administrators.

The backdoor also bypassed the normal WordPress login process, bypassing security measures such as two-factor authentication and login attempt restrictions.

Patchstack's analysis found that the malicious plugins contained a coding error that caused affected websites to return server errors before the backdoor could activate. However, this error didn't eliminate the danger posed by the malicious plugins.

Patchstack identified 99 different names used for the malicious plugins, including one named Site Health Cache. The names generally resembled legitimate website maintenance and performance tools, making them less obvious to website owners reviewing their installed plugins.

WordPress Sites May Be Connected Without Owners Realizing It

An important detail about this security incident is that a website owner might have an active UpdraftCentral connection even if they never intended to use the remote management service.

Patchstack reported that connecting a website to a TeamUpdraft account could automatically create an UpdraftCentral connection because the option to enable remote management was selected by default. Consequently, websites using UpdraftPlus

strictly for backups could have active connection keys without site owners realizing it.

The incident affects websites with active UpdraftCentral Cloud connections, not every website with the UpdraftPlus plugin installed. Patchstack also confirmed that the security issue affected both free and premium versions of UpdraftPlus. TeamUpdraft stated that self-hosted UpdraftCentral installations were not affected.

UpdraftPlus Users Urged To Check Their Websites

TeamUpdraft is urging website owners, including those who have never knowingly used UpdraftCentral, to check their websites for evidence of unauthorized activity.

The company recommends reviewing installed plugins for unfamiliar additions and checking WordPress user accounts for unauthorized administrators.

Website owners should also verify that they are running UpdraftPlus 1.26.13 or 2.26.13, or a newer version, and remove any remaining compromised UpdraftCentral connection keys.

The connection keys can be managed through the WordPress dashboard under Settings, UpdraftPlus, Advanced Tools, and UpdraftCentral.

TeamUpdraft additionally recommends changing administrator passwords and considering restoration from a backup created before October 17 if evidence of compromise is discovered.

Users with TeamUpdraft accounts are also advised to change their account passwords.

The company says there is currently no evidence that attackers retain access to its systems, but its investigation remains

ongoing.

Although the security updates block further access through the compromised connections, they don't remove malicious plugins or unauthorized accounts that may already exist on affected websites. That's why checking for evidence of compromise remains important even after updating.

Featured Image by Shutterstock/Kues

<https://www.searchenginejournal.com/updraftplus-wordpress-plugin-in-security-breach-enables-backdoor-attacks/593909/>