Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

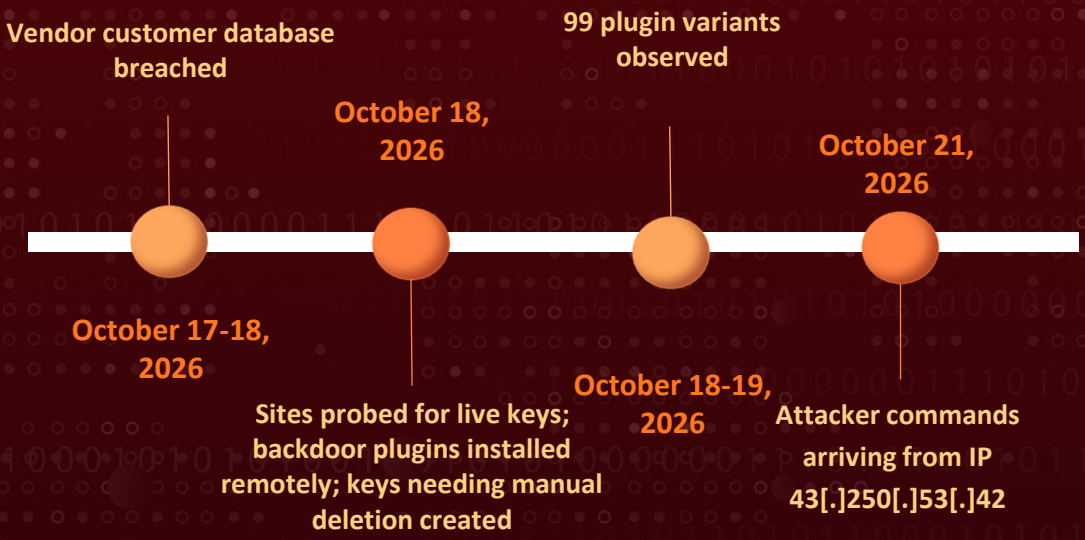
Stolen Keys, Trusted Channel: UpdraftCentral Backdoors WordPress at Scale

Date of Publication	Admiralty Code	TA Number
October 26, 2026	A1	TA2026316

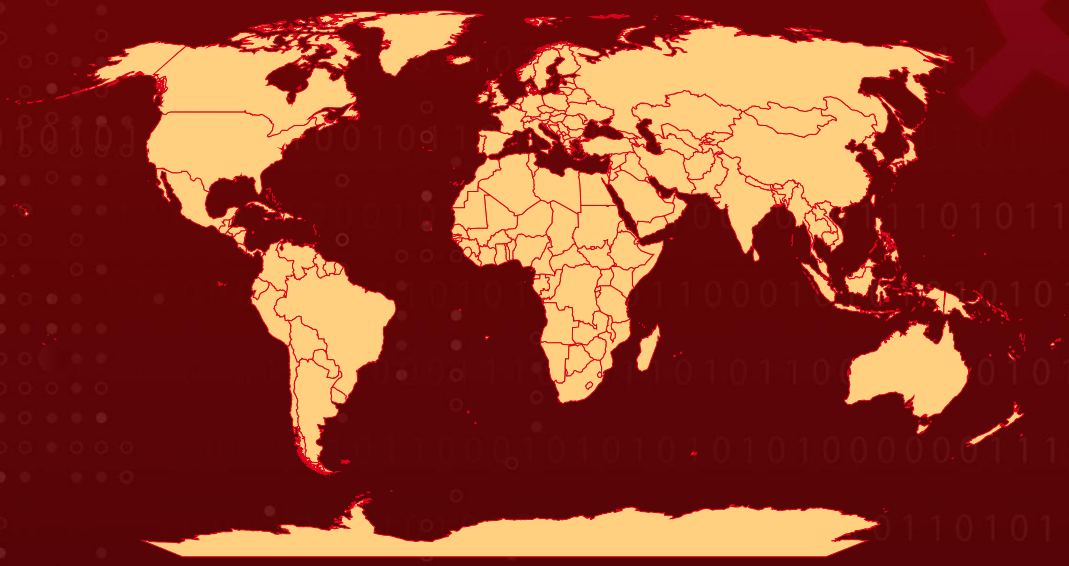
Summary

First Seen: October 17, 2026
Targeted Regions: Worldwide
Targeted Platform: WordPress
Targeted Products: UpdraftPlus (Free and Premium), UpdraftCentral (Cloud), UpdraftVault, UpdraftClone, teamupdraft.com
Attack: An attacker who broke into teamupdraft.com over the weekend of October 17-18, 2026 walked away with the vendor's customer database, including the UpdraftCentral Cloud connection keys that let the service issue signed commands to connected WordPress sites. Within hours, those keys pushed backdoor plugins to sites through the UpdraftCentral channel built into every copy of UpdraftPlus, a backup plugin with more than four million active installations. No vulnerability was exploited on the victim sites: the commands were properly encrypted and signed, so the latest plugin releases accepted them exactly like older ones. The delivered plugins created hidden privileged accounts, logged the attacker straight into wp-admin without touching the login form, and survived removal of the plugin itself.

Timeline



Attack Regions



Targeted Non-Targeted

Attack Details

#1 This attack began at the vendor, not at the websites. Over the weekend of October 17-18, 2026, an attacker broke into teamupdraft.com and reached its customer database. The database held names, email addresses, billing details, order history, hashed passwords, two-factor settings, and UpdraftCentral connection keys. The keys were the real prize. UpdraftCentral lets a central dashboard manage WordPress sites remotely, and its client is built into every copy of UpdraftPlus. Once a site holds a key, it obeys any command signed by that dashboard, and the owner is never asked to approve anything. Many owners did not know they had a key at all, because the box that connects a site is ticked by default and keys never expire.

#2 On October 18, the attacker started testing sites. Each test was a message addressed to a key that does not exist, probe.central.updraftplus.com, and the error that came back showed whether the site was listening. The attacker then sent a signed command to install a plugin, as an ordinary POST request to the site's home page. WordPress installed and activated it with its own installer, so the site recorded a normal plugin install that nobody had asked for. 99 different plugin names were observed over two days, all from the same generator, which changed the name, author, description, password, and secret token for every site.

#3 Every plugin was a backdoor. It checked each visit for a secret web address carrying a long token. When the token matched, the first version created a new user, gave it the Editor role, and quietly added two powers Editors never have: the right to change site settings and the right to install plugins. It then logged the attacker straight into the admin dashboard. Because it set the login cookie itself, the login page was skipped, so two-factor authentication and login limits did nothing. That version had a bug that crashed sites with a 500 error, which is how the first victims spotted it. A second version worked properly and created a full administrator. A third simply logged the attacker in as an admin who was already there, leaving nothing behind in the database, and some versions hid themselves from the plugin list.

#4 After that, nothing more had to be broken. The new account looks like an Editor, so checking the list of administrators does not reveal it. The right to install plugins lets the attacker run any code, and the right to change settings lets them open registration and make every new user an administrator. The account stays behind even if the plugin is deleted, and the attacker knows its password. They also came back more than once. On one site, a broken backdoor was removed and replaced seconds later; some sites received several versions within hours, and commands were still arriving from 43[.]250[.]53[.]42 on October 21. One site was spared only because its key belonged to a user who could no longer install plugins.

#5 The stolen data is the vendor's, not the sites'. Nothing suggests large amounts of data were taken from victim sites, and the loss per site remains unknown. The attacker's traffic ran through the UpdraftCentral channel itself, so it looked almost genuine. The giveaway is the browser name it sent, WordPress/6.4; class-udrpc.php, which is missing the version and web address that real dashboard traffic always includes. The clean-up has been bumpy. Versions 1.26.12 and 2.26.12 were meant to delete the stolen keys, but a bug meant they deleted none, while 1.26.13 and 2.26.13 do the job and were pushed out automatically. A few keys made late on October 18 still must be deleted by hand, and deleting a key removes nothing the attacker has already installed. There is no CVE here, because nothing was broken in the software; the keys were simply stolen.

Recommendations

Check Every Site for an UpdraftCentral Key: Run the check on every WordPress site in your estate, including staging and rarely touched sites, even those where nobody ever deliberately used UpdraftCentral. The connection checkbox is ticked by default when a site is linked to a teamupdraft.com account, so a key may exist without anyone's knowledge. Any output from the updraft_central_localkeys option means the site is exposed.

Update UpdraftPlus to 1.26.13 or 2.26.13, Not 1.26.12: The first emergency release revoked nothing due to a bug. Only 1.26.13 (free) and 2.26.13 (Premium) actually delete pre-incident UpdraftCentral Cloud keys. Confirm the installed version rather than assuming the automatic push from WordPress.org landed everywhere.

Delete Residual Keys by Hand: Keys created on October 18 between 12:07 and 21:00 UTC are not removed even by 1.26.13, so delete every remaining key manually through Settings, UpdraftPlus Backups, Advanced Tools, UpdraftCentral, or by deleting the updraft_central_localkeys option. Removing the site from the dashboard is not enough, because the key that matters lives on the site. Backups continue to work once the key is gone.

Hunt for the Backdoor Account by Capability, Not by Role: The account presents as an Editor, so an administrator-list review will miss it. Query users holding the Editor role together with manage_options or install_plugins, and look for the display name "Site Tools", email addresses at example.org or example.com, and usernames following a two-word-plus-digits pattern.

Sweep Plugin Directories from Disk: Some variants hide themselves from the WordPress plugin screen, so inspect the filesystem rather than the admin UI. Grep plugin directories for the recurring description string "Small maintenance toolkit: keeps option storage tidy.", check the wp-content/upgrade directory where failed installs leave unpacked copies, and treat any plugin by the recurring fake authors as hostile.

Search Access Logs for the Trigger and the Forged User-Agent: Genuine UpdraftCentral traffic carries a library version and vendor URL in its User-Agent; the attacker's does not. Search for POST requests with a bare class-udrpc.php User-Agent, and for GET requests carrying a long hexadecimal parameter with a 32-character value. A 302 response on a trigger request means the backdoor was used, not merely installed.

Remove the Backdoor, Never Repair It: The crashing samples fail only because of a coding error that sits before the token check; fixing the error switches the backdoor on. Delete the UpdraftCentral key first or the attacker will simply push a replacement, then deactivate the plugin and move it out of the web root rather than uninstalling through wp-admin, since its uninstall routine erases its own traces.

Rotate teamupdraft.com Credentials and Remove Stored Passwords: Change the teamupdraft.com password by typing the address directly, reset two-factor settings, and change the same password anywhere it was reused. On Premium sites, clear the account password that UpdraftPlus may still hold in the updraftplus-addons_options database option, including in older backups.

Reconnect Remote Management Under a Least-Privilege Account: If central management is genuinely needed, create the connection under a WordPress user that cannot install or activate plugins. On one analysed site, exactly that detail stopped the attack. Delete UpdraftPlus Migrator keys at the same time, since they use the same channel.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1587: Develop Capabilities	T1587.001: Malware
Initial Access	T1199: Trusted Relationship	
	T1078: Valid Accounts	
Execution	T1072: Software Deployment Tools	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1136: Create Account	T1136.001: Local Account
Privilege Escalation	T1098: Account Manipulation	T1098.007: Additional Local or Domain Groups

Tactic	Technique	Sub-technique
Stealth	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1564: Hide Artifacts	
Lateral Movement	T1072: Software Deployment Tools	
	T1550: Use Alternate Authentication Material	T1550.004: Web Session Cookie
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	43[.]250[.]53[.]42, 178[.]83[.]37[.]220, 178[.]83[.]37[.]243, 178[.]94[.]218[.]31, 107[.]189[.]14[.]87, 45[.]61[.]188[.]240, 45[.]61[.]184[.]170
IPv6	2a09[:]bac5[:]4e21[:]2e3c[::]49b[:]9
Hostname	probe[.]central[.]updraftplus[.]com, 0[.]central[.]updraftplus[.]com
Email	data-ops43[@]example[.]org, render-build21[@]example[.]org, wp[.]tech506[@]example[.]com

TYPE	VALUE
SHA256	3c3355f7692d4951e565568378379557946 7c9bf1ae2152e13b8c80e9021209f, 4186ae2aa0472a4e7929b21bb87f9b61866cb3790f69f4b6c9813e196955d5f0, bb40f9a87cea678aa50e5286dd91c0903d6a7fc1b12391472187a0919b4d0801, 4943fc21efa4b81516130f92bf4efe3b832e1bb69e499d2e42587233a0a005e9, a9b625496a8ec82862ded01900f720c28f111e624176df7e25be7331f22e4cc9, 325722876a5f8e184b88cf415900ab52c9103553bc4be502399a2272550f2111, 0290c2baa363eac72ef2b6891bef1c9c8b4774d5b95d14f4871bde6094fdacde, 99a7fb44d1502938a40b3f663f4e5771b5cf741bcbaec58d7dda0b5066b5a0a5, 03301b6fc563cafe0408a7eec0fee0349188ff95ce3e5e458272ff6fb23c6a63, 8cdd7ab6d232976a6763df93324be7182a24427e0582fec1dd3c85fc120b8190, 8ff28a902ce6ae9897260ee8a3c90150ab4301946b4ad8f7247c6b8c9c99f321, 6a52fed5e4044978b68dc70bbabef127369c59ec63661e7478bd5c4ac781cf30, 80ba1b6261e573a632451aa77485f78739fbdd13ffccaeafbbe91ee2852f8483, 0d9941f42e3c191b68f80ca0f4f1702c99ad8c6633508a6e01b82973d96a71a3, d3281d662c017882d29a7d47412c629a332aba09ac4a04489a28cbdccd7f90a8, 7376a09d1281f27fa58c72811e4c28075ae16a353315d249e4840841cf0225f2, 02f5338311a5b5ab443dae447fddbb8885c86f4c16cfa9bd984582c2777b5429, 425bb1e680d57a92327c99090df1e3b69932c4ec3d9c22f105d89b101f412d72, 335dc74431648b713500db50d2beafda19342555ba19e37438df035f802c6017, 59231b0e5004672b3058b47b4b4ff2b1fa89f1961bedf1741ba285e8adbe4928, 54ca7b2da87852a5d1fd7bde644027f84557db4d45fbb25cb2d135a3497d8d5c, 2cdf3f2a3f10f0e12f00f2267907d44796107ab4aececdac520bba13e012b47a, 1821a58e2a851acd1a608a77ce2f77817a0b7b6ef344b9889c8f8728e62969ec,

TYPE	VALUE
SHA256	43dc88fd18501be3dbd6d7f1755e77386d081dd41cef82bc514d39991ae69c49, fd664098cf189698e730b94fe1ea9f4425738f1be4bb9bd19eb38e14dbdf72e1, 0f194a46d99a8180908a55d1ae9d5bb51e9257e68ba10312ce030b8a5cd2c8dd, 87cb01de622d0108b60d4f3d6663935a7b53fd17b6b82b53a26e47a5b522dc91, ca5ba1b02d4f1802c8182e7a71a4668959f42b501c523864c48dfdfc03ad54e8, 056db22ebb8b1c0036a992ecf9c37c7f868b1eab68812445eed29062fc2307fa, fd37eda3283416c568d53dd437f190341221138d8efabc7437e983b09946f9dd, 2fc98e80960d196fa5b70ffa8c76ee5332c9d6c60465fe2e38ab2c597c357205
File Path	wp-content/plugins/<backdoor-slug>/, wp-content/upgrade/, wp-content/mu-plugins/
User-Agent	WordPress/6.4; class-udrpc.php, Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
HTTP Request	POST / (udrpc_message parameter present), GET /?<trigger-parameter>=<32-character-token>
Filename	load-stack-35c, text-gantry-eb0, hero-frame-2c5, card-binder-104, style-bridge-8f5, media-kit-183, query-shelf, post-dock-776, nav-hub,

TYPE	VALUE
Filename	speed-desk, speed-kit-300, link-latch, script-shelf, feed-case, cache-jack-c7a, src-lab, render-helper-232b, opt4fix, js-fix-757a, lazy-tool-3055, cache-smith, boost-kit, fast2engine, defer-engine, minify-tool-bf90, site-health-364f, site-health-cache, speed-press-23b, hero-bridge-6c9, site-health-6a20, db-works-7dba, cache-frame, site-engine
Username	data-ops43, media-staff96, render.desk87, data.build20, web_maint88, site_build55, render.maint85, data-team4, media.crew54, content-crew90, web_ops15, render.desk2, system_team850, web.tech988, cmseditor170, cms.tech644, web_mgr684, media-mgr138, pageeditor85, wp.tech506, site_editor784, site.crew51, web_desk9

References

https://patchstack.com/articles/updraftcentral-key-compromise-wordpress-backdoors/

https://www.wordfence.com/blog/2026/10/updraftcentral-connection-key-compromise/

https://www.rescana.com/post/updraftcentral-stolen-keys-wordpress-backdoors-october-2026

https://nethemba.com/updraftcentral-backdoor-analysis/

https://teamupdraft.com/blog/security-incident-october-2026/

https://www.jacobtyler.com/blog/wordpress-plugin-supply-chain-attack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

October 26, 2026 • 09:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com