

Rank Math PRO plugin downloads briefly carried a backdoor in a supply-chain attack



Some downloads of Rank Math PRO 3.0.123 from the vendor's site contained malware over an 11-hour window. Sites that activated it should be treated as compromised and cleaned, not just updated.

- Version 3.0.123 of Rank Math PRO, downloaded from the official site between October 15 (20:02 UTC) and October 16 (07:12 UTC), could contain malware.
- The free Rank Math SEO plugin from WordPress.org was not affected.
- The malware keeps persistent access, contacts rank1cdn[.]com and recreates hidden backdoors when the site is visited.
- Database credentials, API keys and other secrets reachable by the web server may be exposed.
- Updating or deactivating the plugin does not remove the threat; the clean release is 3.0.124.

The vendor of Rank Math PRO, a paid WordPress SEO plugin, reports that a limited number of users who downloaded version 3.0.123 from its official website received a trojanized copy. The window ran from October 15 at 20:02 UTC to October 16 at 07:12 UTC, roughly 11 hours. The vendor has removed the affected files and released a clean version, 3.0.124.

What the malware does

According to the vendor, the malware establishes persistent access, communicates with rank1cdn[.]com and rebuilds hidden backdoors whenever someone visits the infected site. Secrets accessible to the web server, such as database credentials and API keys, should be considered exposed.

BleepingComputer also found a PHP sample on VirusTotal that shares indicators with the vendor's alert, including administrator-account creation using the 'wpsupport_' prefix. It appears to be a first-stage script that can run commands, modify WordPress databases and steal cloud credentials and SSH keys. BleepingComputer could not confirm that it was delivered through the plugin. The vendor had not answered questions on the number of affected sites or the initial attack vector.

Cleanup guidance

Sites that installed and activated the affected version should be treated as compromised. The recommended route is to restore files and database from a clean backup, scan, and rotate all passwords, keys and salts. Without a safe backup, manual cleanup is needed: delete the whole plugin folder and malicious database entries, then look for other backdoors, unauthorized administrators, altered files, scheduled tasks and changes outside WordPress. Outbound connections to rank1cdn[.]com should be blocked.

If the plugin was installed but never activated, delete it, download 3.0.124 and scan the site.

What to do now

1. Check whether any website, including those run by agencies or vendors, uses Rank Math PRO and which version was downloaded between October 15 and 16.
2. Treat any site that activated 3.0.123 as compromised: restore from a clean backup or clean manually, as the vendor advises, and do not rely on updating alone.
3. Rotate database credentials, API keys, cloud keys, SSH keys, passwords and WordPress salts reachable from affected servers.
4. Review administrator accounts (such as 'wpsupport_' usernames), scheduled tasks and changed files, and block outbound traffic to rank1cdn[.]com.
5. Record the event under your incident and third-party risk processes, and delete and replace the plugin with 3.0.124 where it was installed but never activated.