

Rank Math PRO WordPress Plugin Distributed Malware in a Short Window on 15–16 October



Rank Math says copies of Rank Math PRO downloaded or updated between 20:02 UTC on 15 October and 07:12 UTC on 16 October contained malware. Sites that installed and activated them should be treated as compromised.

- Affected copies were those downloaded from rankmath.com or delivered as updates between 20:02 UTC on 15 October and 07:12 UTC on 16 October.
- Rank Math published a security notice on 16 October.
- Any site that installed and activated an affected copy should be treated as compromised.
- The headline describes the malware as a self-restoring backdoor; the excerpt available gives no further technical detail.

Rank Math, the vendor of the Rank Math SEO plugin for WordPress, has disclosed that copies of its paid Rank Math PRO product contained malware for a limited period.

What happened

According to the vendor's security notice of 16 October, any copy downloaded from rankmath.com, or delivered as an update, between 20:02 UTC on 15 October and 07:12 UTC on 16 October was malicious. The reporting headline describes the payload as a self-restoring backdoor, which suggests that removing a single file may not be enough to clean an affected site. The excerpt we reviewed does not explain the mechanism in detail.

Who should act

The vendor's guidance, as reported, is that any site that installed and activated one of these copies should be treated as compromised. Organisations that run WordPress sites with Rank Math PRO, directly or through a web agency, should first establish whether an update or download occurred inside the stated window.

Practical view

The exposure window is under twelve hours, so many sites will be unaffected, but the only reliable way to know is to check update and download records. Where there is a match, treat it as an incident rather than a routine plugin issue, and follow the vendor's notice for specific remediation steps. Do not rely on simply deleting or updating the plugin, given the self-restoring behaviour described.

What to do now

1. Inventory all WordPress sites, including those run by agencies, and identify which use Rank Math PRO.
2. Check update logs and download records for installs between 20:02 UTC on 15 October and 07:12 UTC on 16 October.
3. Treat any site that installed and activated an affected copy as compromised and open an incident under your response process.
4. Follow the remediation steps in Rank Math's 16 October security notice.
5. Review third-party and agency arrangements for how plugin updates are vetted and approved.