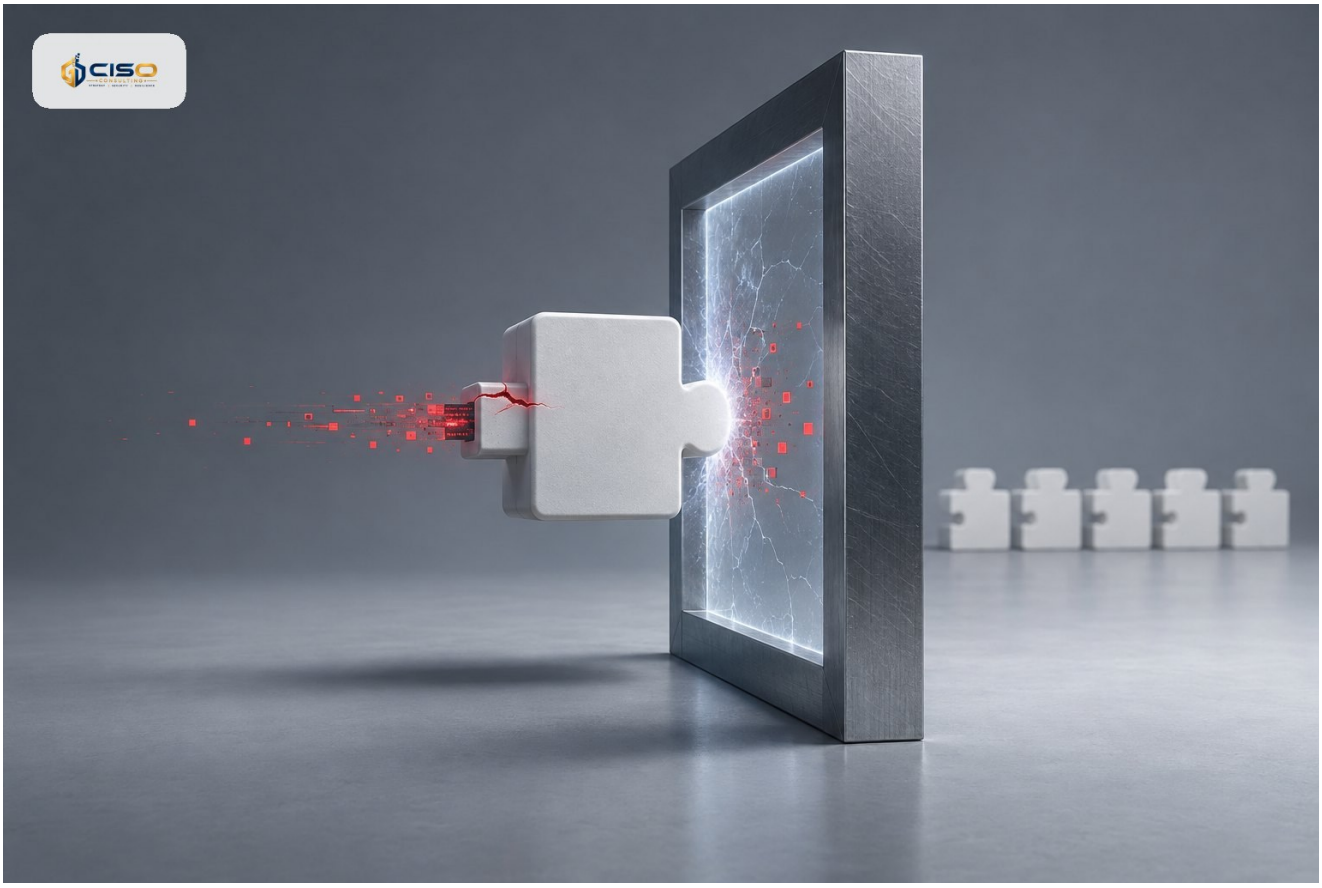
WordPress Blocks Six Backdoored WP Connect Plugins Before Release



WordPress removed six WP Connect plugins that were backdoored on November 22, 2026 to allow arbitrary code execution, after a suspected developer account compromise. The plugins team blocked the malicious releases before they went live.

- Six plugins by WP Connect were removed from WordPress.
- They were backdoored on November 22, 2026 to enable arbitrary code execution.
- The cause is a suspected compromise of the developer's account.
- The WordPress plugins team detected the threat independently and blocked it before official release.
- Plugin listings are now unavailable.

What happened

WordPress has removed six plugins developed by WP Connect. According to the report, the plugins were backdoored on November 22, 2026, in a way that would allow arbitrary code execution on any site running them. The suspected cause is a compromise of the developer's account.

The WordPress plugins team detected the activity on its own and blocked the malicious versions before they could be officially released. The plugin listings are now no longer accessible.

Why it matters

This is a supply-chain risk: a trusted publisher account is used to push harmful code through a normal update channel. Arbitrary code execution on a web server can lead to site takeover, data exposure and a foothold in the wider network.

The source does not name the six plugins, say whether any site was affected, or describe how the account was compromised. Institutions should therefore verify their own exposure rather than assume none.

Recommended approach

The priority is to confirm whether any WP Connect plugin is installed on corporate, subsidiary or agency-managed WordPress sites, and to treat any finding as a potential incident until shown otherwise. Longer term, plugin and publisher account security should be part of third-party and change management.

What to do now

1. Inventory all WordPress sites, including those run by agencies, and list installed plugins.
2. Check for any WP Connect plugins and remove or disable them.
3. If found, review for unexpected code, admin users, scheduled tasks and outbound connections, and follow incident response procedures.
4. Rotate credentials and keys on any affected site.
5. Add plugin vetting and update review to third-party and change management processes.