Refugee Ball

Security case study — refugeeball.org.au

Sector	Refugee-health charity (AU)
Platform	WordPress (Salient)
Scope	Database + File
Attack family	Rotating fake-plugin dropper
Entry vector	Unpatched Salient Core/Shortcodes vulnerability
Verdict	CRITICAL Critical

> **Active fake-plugin backdoor + rotating dropper → cleaned & verified**

The problem

This refugee-health charity's site had an active backdoor disguised as a caching plugin, plus a second fake “media engine” plugin that had been deactivated the day before the export — the signature of a rotating-dropper reinfection scheme designed to keep swapping in fresh backdoors. The way in was an unpatched, known vulnerability in the site's Salient theme components that had been ignored.

What I did

- Confirmed the active fake caching plugin as a backdoor and identified the recently-deactivated second fake plugin as evidence of dropper rotation.
- Pinned the entry vector to the unpatched Salient Core and Shortcodes vulnerabilities, and noted that Wordfence had indexed the fake-plugin files without flagging them as malware.
- Verified the file backup was clean (the fake plugin folders already removed) and confirmed the six user accounts were all legitimate with no injected scripts or spam.
- Verified the re-optimised, cleaned database export as clean across users, scripts, spam, payloads, cron, and suspicious domains — with only cosmetic security-tool history left behind.

The result

The charity got a clear before-and-after: an infected database with the backdoor named and located, a clean file system, and a verified-clean database after cleanup — three reports in total. I was careful to keep the still-open server-level work explicit: patch the Salient entry vulnerability,

rotate every credential, and harden, because a clean database does not by itself make the site immune.