SICHERHEITS-CHECKLISTE

Ist deine WordPress-Seite von "wp2shell" betroffen?

Eine kritische Sicherheitslücke im WordPress-Core (CVE-2026-63030 & CVE-2026-60137) erlaubt Angreifern die vollständige Übernahme einer Website – ganz ohne Passwort. Diese Checkliste zeigt dir in 7 Schritten, wie du herausfindest, ob du betroffen bist, und wie du sicher updatest.

500 Mio.+
Websites weltweit potenziell betroffen

Critical
Offizielle Einstufung von CVE-2026-63030

Aktiv
Von CISA als aktiv ausgenutzt gelistet

☐ 1. WordPress-Version herausfinden

Im Backend unter *Dashboard → Startseite* oder *Dashboard → Updates*. Ohne Login: Seitenquelltext (Strg+U) nach "generator" durchsuchen, oder *deineseite.de/feed/* aufrufen – dort steht die Version meist im Quelltext.

☐ 2. Prüfen, ob deine Version betroffen ist

Betroffen	6.8.0–6.8.5 | 6.9.0–6.9.4 | 7.0.0–7.0.1
Sicher	6.8.6 | 6.9.5 | 7.0.2 oder neuer

☐ 3. Vor dem Update: Backup erstellen

Kein Update ohne Backup – das wird am häufigsten übersprungen. Zwei Ebenen sichern:

- Dateien (Backup-Plugin wie UpdraftPlus, oder über den Hoster/FTP)
- Datenbank (meist im gleichen Plugin enthalten, sonst per phpMyAdmin-Export)

Backup extern speichern – nicht nur auf dem gleichen Server.

☐ 4. Update durchführen

Unter *Dashboard → Updates* anstoßen. Wenn möglich vorher auf einer Staging-Umgebung testen (viele Managed-Hoster bieten das mit einem Klick). Ohne Staging: Update in einem ruhigen Zeitfenster einspielen, nicht während Stoßzeiten.

☐ 5. Nach dem Update: Funktionscheck

Startseite, Kontaktformular, Checkout (falls Shop) und Backend kurz durchklicken. Bei Elementor-Seiten zusätzlich: ein bis zwei Seiten im Elementor-Editor öffnen und prüfen, ob sich alles normal bearbeiten lässt – Konflikte zwischen Core-Update und Page-Builder-Widgets sind der klassische Stolperstein.

☐ 6. Falls ein Update gerade nicht möglich ist

Übergangsweise per Sicherheits-Plugin (z. B. Wordfence, Sucuri) den REST-API-Pfad */wp-json/batch/v1* blockieren oder die REST-API für nicht angemeldete Nutzer einschränken. Das ist eine Notlösung, kein Ersatz fürs Update.

☐ 7. Wichtig: Elementor & andere Page-Builder schützen nicht

wp2shell sitzt im WordPress-Core – unabhängig davon, ob du Elementor, Divi oder gar keinen Page-Builder nutzt. Entscheidend ist ausschließlich die Core-Version. Page-Builder-Plugins wie Elementor hatten 2026 zusätzlich eigene, separate Sicherheitslücken – ein Update auf die jeweils aktuelle Plugin-Version lohnt sich also zusätzlich.

Anzeichen, dass es bereits zu spät sein könnte

Unbekannte Dateien im Plugin- oder Theme-Ordner · neue Admin-Benutzer, die niemand angelegt hat · auffällige Log-Einträge rund um */wp-json/batch/* · plötzlich langsame oder seltsam reagierende Seite. In diesem Fall reicht ein Update allein nicht mehr – dann braucht es eine echte Bereinigung.

Unsicher, ob deine Seite betroffen ist?

Ich prüfe kostenlos und unverbindlich, welche WordPress-Version bei dir läuft, ob du betroffen bist – und wie du sicher updatest, ohne dass danach etwas kaputtgeht.

office@digital-wannabeez.at

Quellen: CERT.at, Rapid7, ACA Group, Qualys ThreatPROTECT, Patchstack, WPScan (Stand: August 2026). Diese Checkliste ersetzt keine individuelle Sicherheitsanalyse.