SOFTWARE HOLES · CHECKLIST

3 Close the side doors

From the lesson: The side doors: plugins, add-ons and old software

Works for WordPress, Joomla and Drupal. Builder users: see the last two items.

THE PATTERN

- Each plugin, theme or app is someone else's code, and a possible door.
- Once a hole is public, robots try it within hours.
- Abandoned, "free paid" (nulled) and recently sold plugins are the riskiest.

HOW TO SPOT IT

- "Update available" badges that have sat there for weeks.
- Plugins or apps you don't remember adding.
- A plugin that hasn't been updated by its maker in over a year.
- A plugin that changed owner or name recently.

TICK AS YOU GO

- [ ] **List every plugin and theme**
  WordPress: Plugins, then Installed Plugins, and Appearance, then Themes. Write down the count.
- [ ] **Delete what you don't use**
  Deactivate, then Delete. Keep one spare default theme and delete the rest.
- [ ] **Replace anything abandoned**
  If a plugin page says it hasn't been updated in over a year, or it was closed, look for an alternative.
- [ ] **Remove any "free" copies of paid plugins**
  If you didn't buy it from the maker, assume it's unsafe. Replace it with the genuine version.
- [ ] **Turn on automatic updates**
  WordPress: Enable auto-updates on each plugin and theme. Ask your host to keep the PHP version current too.
- [ ] **Builders: review connected apps**
  Wix: Apps. Squarespace: Extensions. Shopify: Apps. Remove anything you don't use.
- [ ] **Builders: check pasted code**
  Look in custom code, header or embed settings for tracking or widget code you no longer need.

REMEMBER Every add-on is a door. The safest door is one you've removed.

11,334 new security holes found in WordPress add-ons and themes in 2025, up 42% (Patchstack).

hedgehog.site · © 2026 Hedgehog Site Limited