WordPress Plugin Vulnerability Alerting

mySites.guru cross-references every WordPress plugin on your sites against Wordfence, CVE and custom threat databases, flagging vulnerable plugins instantly.

Phil E. Taylor | 26 March 2026

Outdated plugins are the most common way WordPress sites get compromised. If you suspect a vulnerable plugin has already been exploited, check whether your site has been hacked first - and if it has, the WordPress hacked recovery guide covers what to do next. mySites.guru checks every plugin version on your connected sites against known vulnerability databases and flags the ones that need attention.

How does WordPress vulnerability detection work?

The mySites.guru snapshot runs twice a day on each connected site, collecting a list of every installed plugin and its version number.

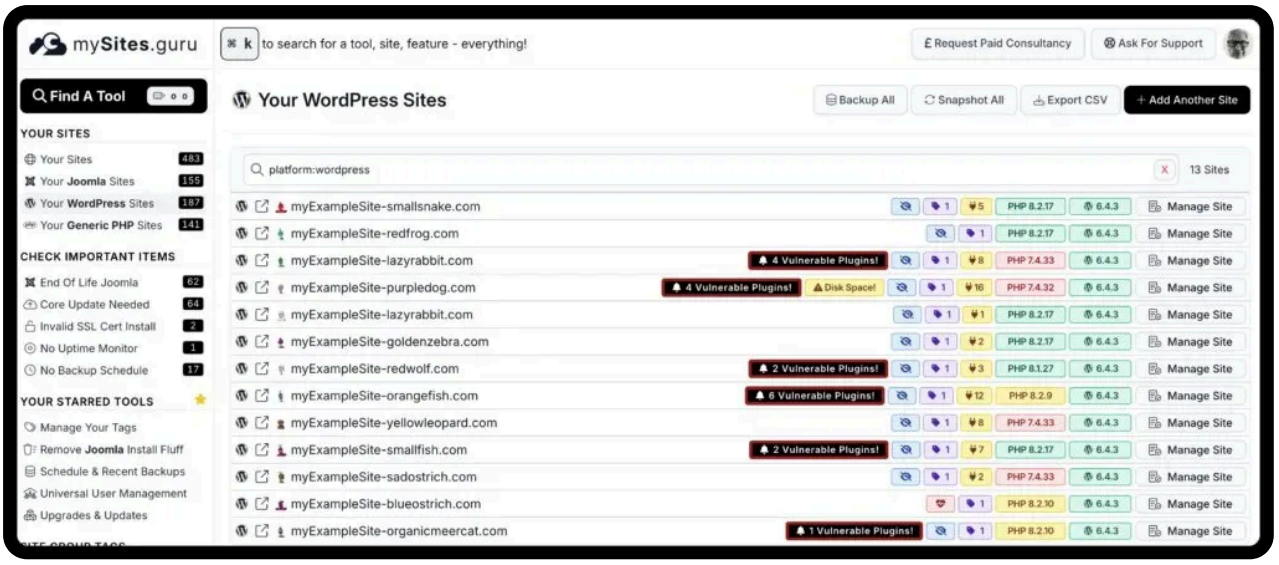
That list gets compared against several threat intelligence sources:

- Wordfence vulnerability data
- CVE and Mitre datasets
- Custom vulnerability lists and internal threat data built up over 12+ years

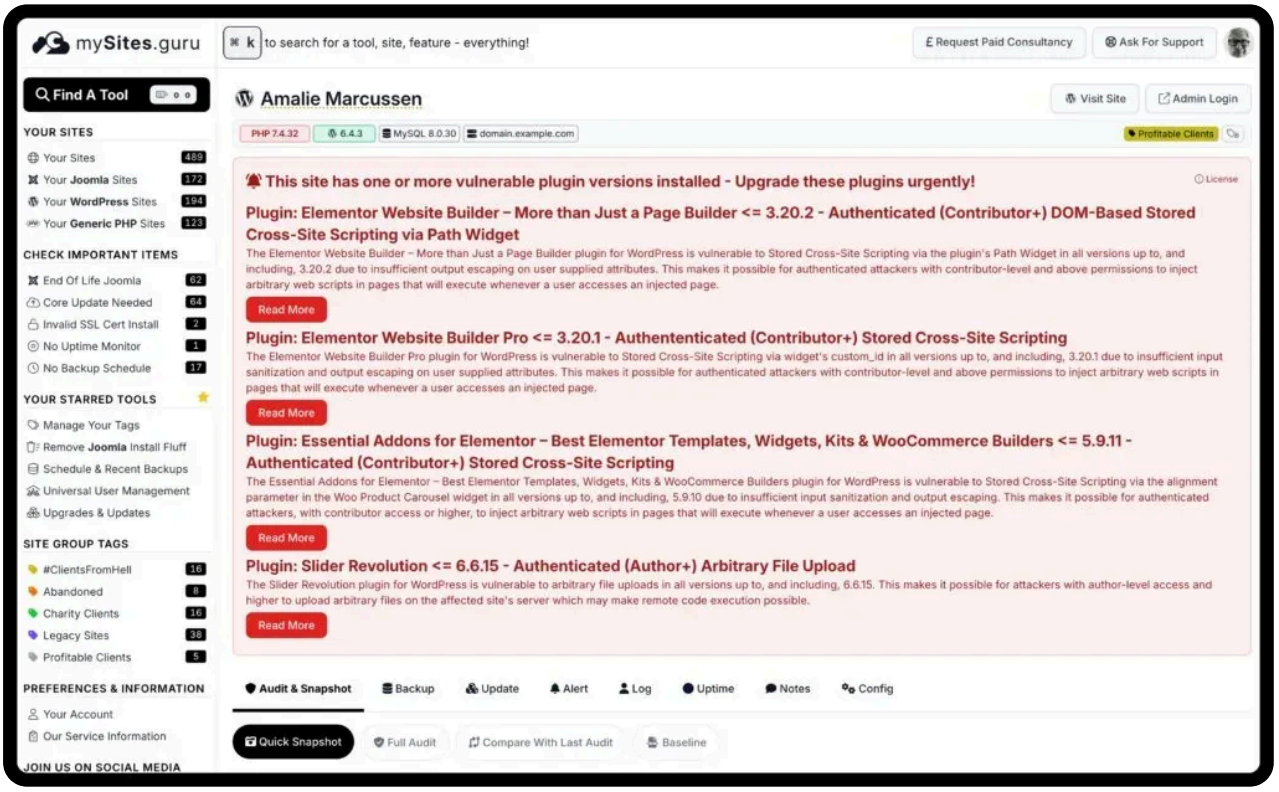
If a plugin version on your site matches a known vulnerability, it gets flagged immediately. A recent example: the Smart Slider 3 arbitrary file read vulnerability affected over 800,000 installs and was picked up automatically for any connected site running a vulnerable version.

What do WordPress vulnerability alerts look like?

On the main sites page, vulnerable sites are marked so you can spot them at a glance:



Click into an individual site and you get the specifics - which plugins are affected, what the vulnerability is, and a link to the full disclosure:



How do you fix vulnerable WordPress plugins?

In most cases, updating the plugin to the latest version is the fix. Plugin authors typically patch vulnerabilities in new releases, so staying current is the single best thing

you can do.

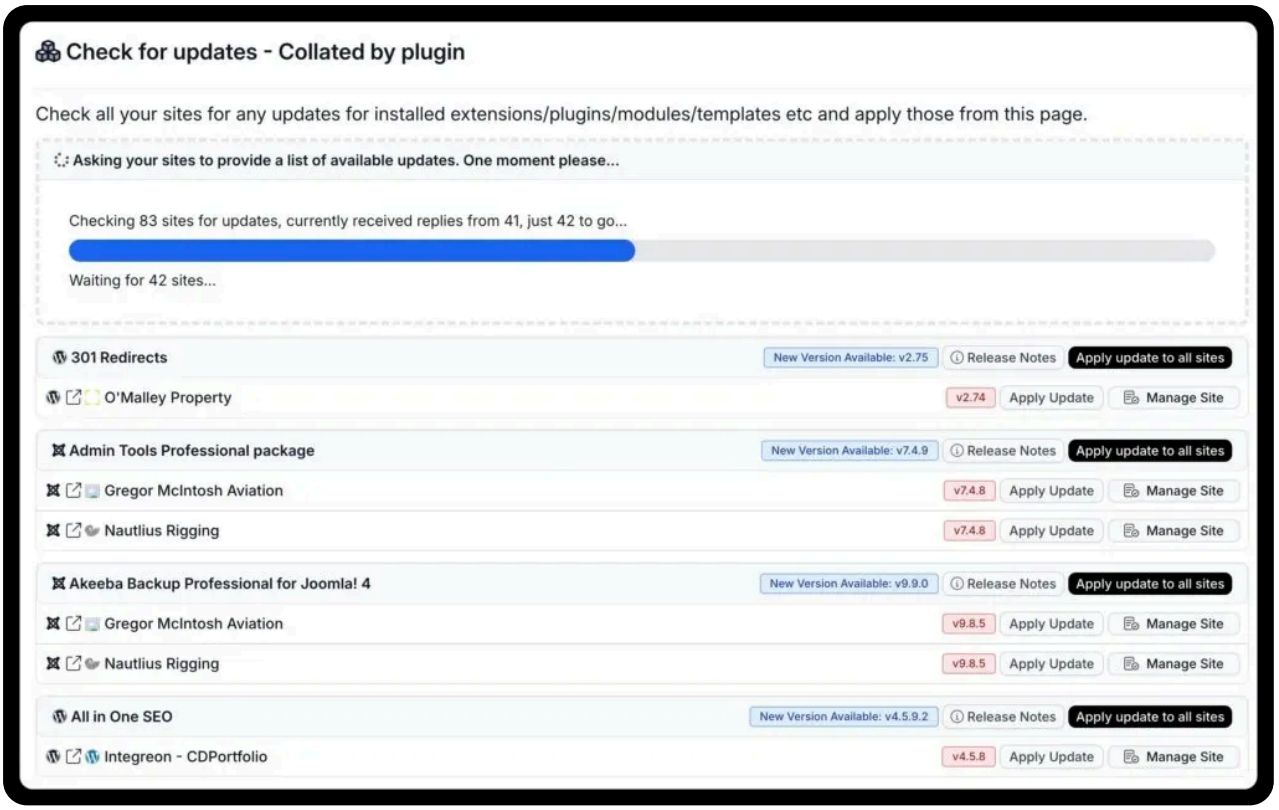
The best practice checks in mySites.guru will also flag other security hygiene issues - outdated PHP versions, debug mode left on, missing security headers - that compound the risk from vulnerable plugins. You should also enforce minor-only core updates so that WordPress keeps applying security patches without risking a major version jump that breaks plugin compatibility.

> ⚠️ **What about zero-days?**
>
> Zero-day vulnerabilities have no public disclosure yet, so no scanner can catch them before they're known. Once a vulnerability hits Wordfence, CVE, or another public database, mySites.guru picks it up on the next snapshot cycle - typically within 12 hours.

How do you update vulnerable WordPress plugins across all your sites?

Finding the vulnerability is half the job. Fixing it across 50 or 200 sites is where the time goes. If you've disabled automatic updates to keep control over what runs on your sites, you'll want to push vulnerable plugin updates manually as soon as a patch is available.

The mass plugin updater lets you select every site running a vulnerable plugin version and push the update in one batch:



You can also mass install a replacement plugin if the vulnerable extension has been abandoned and you need to swap it out entirely.

What do you do when a WordPress plugin has no patch available?

Sometimes a vulnerability gets disclosed before the author releases a fix. In that case:

- **Deactivate the plugin** on affected sites if it's not critical to functionality
- **Set up** real-time file alerts so you'll know immediately if someone exploits it
- **Run a** security audit to check whether the vulnerability has already been used - or use the WordPress malware scanner for a focused scan
- **Monitor the plugin's changelog** - mySites.guru will automatically clear the alert once an updated version is installed

If the plugin stays unpatched for an extended period, that's usually a sign it's been abandoned. Time to find an alternative.

Why does WordPress plugin security matter at scale?

One WordPress site with one vulnerable plugin is a manageable risk. But if you're managing 100+ client sites with 15-20 plugins each, that's a lot of versions to track. Nobody's doing that by hand. The WordPress vulnerability scanner page covers exactly how mySites.guru handles this at scale, with detail on the threat databases and detection cycle.

mySites.guru runs these checks automatically, twice a day, across every connected site. When something needs attention, you see it on your dashboard - not three months later when a client calls to say their site is defaced.

Run a free audit on any WordPress site to see what mySites.guru finds.

Vulnerability management is a key part of our agency security guide.

Frequently Asked Questions

How does mySites.guru detect vulnerable WordPress plugins?

Twice daily, mySites.guru snapshots each connected site's installed plugin versions and cross-references them against Wordfence, CVE/Mitre, and custom threat intelligence databases.

How do I fix a plugin flagged as having a known vulnerability?

In most cases, updating the plugin to the latest version resolves the vulnerability. If no patch exists yet, consider deactivating the plugin until one is released.

Can I update a vulnerable plugin across multiple WordPress sites at once?

Yes - the mass plugin updater in mySites.guru lets you select and apply plugin updates across many WordPress sites in a single operation.

Does mySites.guru check for zero-day vulnerabilities?

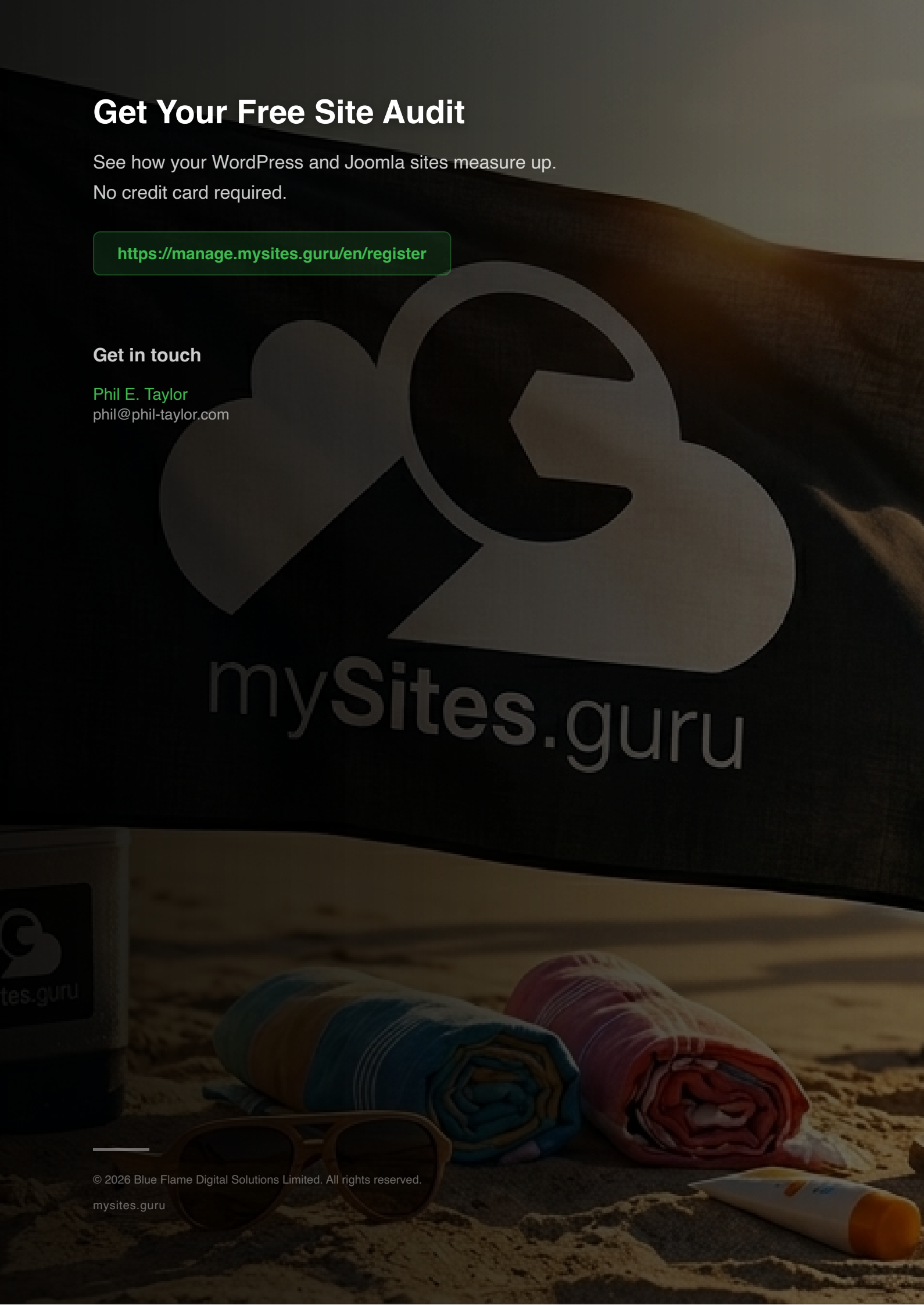
Not directly - zero-days by definition have no public disclosure yet. But once a vulnerability is published to Wordfence, CVE, or other databases, mySites.guru picks it up on the next snapshot cycle.

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

https://manage.mysites.guru/en/register



Get in touch

Phil E. Taylor
phil@phil-taylor.com