mySites.guru

Regular Labs Patched Its Whole Joomla Extension Catalogue at Once

Regular Labs shipped a security-hardening update across its Joomla extension range on 22 July 2026: SSRF, command injection, stored XSS and more. No CVEs.

Phil E. Taylor | 26 August 2026

Regular Labs, the one-developer Joomla shop Peter van Westen has run since 2010 (you may remember it as NoNumber before the 2016 rebrand), is one of the most widely installed names in the ecosystem. The vendor says its extensions run on more than 100,000 websites, and on our own account the shared Regular Labs Library alone sits on more than 16,000 of the Joomla sites we manage, with household-name extensions like Advanced Module Manager, Sourcerer, Articles Anywhere and Cache Cleaner on thousands each. On 22 July 2026 Regular Labs pushed a security-hardening update across roughly 30 of those extensions at once, and did it quietly: no separate advisory, no CVE numbers, just a stack of changelog entries tagged `[SECURITY FIX]`.

That combination, huge install base and a low-key rollout, is exactly how a release like this gets missed. If you run any Regular Labs extension on a Joomla site, update it now. If you manage more than a handful of sites, read on for how to find every affected one at once.

mySites.guru already flags the affected sites

You do not have to read 30 changelogs and cross-check them against every site by hand. mySites.guru keeps a live inventory of every extension on every connected Joomla site, and we have added detection rules for the vulnerable versions of the higher-risk extensions in this release. Any connected site still running an affected version is flagged automatically, with the exact version it is on and whether the fix is available.

See every Regular Labs extension across your sites

Open your Extension Inventory

Search for Cache Cleaner, Sourcerer or any Regular Labs extension across every connected Joomla site and filter for outdated versions. Not a subscriber? Sign up free and connect your sites.

TL;DR

- Regular Labs shipped a **coordinated security-hardening update across roughly 30 Joomla extensions** on 22 July 2026
- **Two fixes are in the shared Regular Labs Library**, so they affect every one of their extensions: privileged AJAX endpoints that did not consistently enforce tokens and permissions, and a bundled HTTP-message library updated to close a request start-line injection
- **Cache Cleaner** fixed the most serious set: server-side request forgery to private networks, an OS command injection reaching a shell command on SiteGround hosts, path traversal and credential exposure
- **GeoIP** fixed unauthenticated client-IP header spoofing that can bypass GeoIP-based access rules and Conditions
- The **Articles, Modules and Users Anywhere** content plugins fixed SSRF via external image downloads, stored cross-site scripting and exposure of restricted content and authentication data
- **Modals** and **Tooltips** fixed stored XSS through decoded HTML; **Keyboard Shortcuts** stopped shortcut overrides running arbitrary JavaScript; **Sourcerer 13.0.0** restricts PHP in articles to Super Users
- **Sourcerer needed a second release.** On 17 August 2026, Sourcerer 14.0.0 closed the other half of the same problem: 13.0.0 checked the origin of code in articles, but nowhere else in the page. Every 13.x build is affected
- **No CVEs were assigned.** These are Joomla **extension** issues, not Joomla core
- **Update every Regular Labs extension you run.** mySites.guru already flags every connected site still on a vulnerable version

What Regular Labs actually shipped

Two of the security fixes in this release are not in any single extension. They are in the Regular Labs Library, the shared framework that every Regular Labs extension

installs and loads, which is why the same two lines appear at the bottom of nearly every changelog.

The first is that Regular Labs' **privileged AJAX endpoints did not consistently enforce valid tokens, matching permissions, and trusted form configuration**. AJAX endpoints are the quiet back door of CMS security: they are reachable over the web, they are easy to forget when you audit permissions, and a missing token or capability check turns an administrator-only action into something a lower-privileged user, or a forged cross-site request, can trigger. We wrote about why AJAX endpoints are a CMS security blind spot before this release, and it is the exact pattern being hardened here across the whole catalogue.

The second is a **bundled HTTP-message library updated to fix a request start-line injection**. Regular Labs extensions that make outbound HTTP requests ship a copy of a PSR-7 message library, and a carriage-return or line-feed smuggled into the request line, protocol version or reason phrase without validation can inject extra headers or split a second request. The changelog names neither the library nor a CVE, but the wording lines up closely with a known issue in the widely-used `guzzlehttp/psr7` package, CVE-2026-55766, a CRLF injection in HTTP start-line serialization fixed in psr7 2.12.1 and disclosed in June 2026. We cannot confirm from closed source that this is the exact dependency Regular Labs bundles, but the description matches. It is a lower-priority fix for most sites, and it travels with every extension you update.

Beyond those two, most of the release is administrator-side hardening: adding the token or permission check that should have gated an admin route, escaping stored values before they render in the admin, rejecting SQL comment and write keywords in DB Replacer's custom filters. Important, but exploitable mainly by someone who already has an account. The issues worth prioritising are the handful that reach further.

Which Regular Labs extensions have the serious fixes?

A few extensions fixed issues that an unauthenticated visitor, or a low-privilege user, can reach. These are the ones to update first.

Extension	Fixed in	The issue that matters
Cache Cleaner	10.0.0	SSRF to private/reserved networks, OS command injection (host value to shell on SiteGround), path traversal, CDN credentials exposed in admin URLs
GeoIP	7.0.0	Unauthenticated client-IP header spoofing bypassing GeoIP access rules; SSRF, credential exposure and unsafe archive extraction on database update
Articles Anywhere	19.0.0	SSRF via external image downloads, stored XSS through tag HTML, restricted/unpublished content and authentication data exposure
Modules Anywhere	9.0.0	Stored XSS, module access and publication bypass, module data exposed to unauthorised logged-in users
Users Anywhere	2.0.0	SSRF via external image downloads, stored XSS, authentication and restricted contact data exposure
Modals	16.0.0	Stored XSS through decoded modal HTML; gallery folder path traversal
Tooltips	10.0.0	Stored XSS through decoded tooltip HTML
Keyboard Shortcuts	4.0.0	Shortcut action overrides accepted arbitrary inline JavaScript
Sourcerer	13.0.0	PHP in articles restricted to Super Users; CSS/JS/PHP permissions enforced across article creators and modifiers

Cache Cleaner is the one to update first

Cache Cleaner runs on more of the sites we manage than any other Regular Labs extension in this release, and it fixed the widest set of issues. The standouts are a **server-side request forgery** where custom query URLs could reach private or reserved network services, and an **OS command injection** on SiteGround hosts where a request host value could reach a shell command. It also closed a path traversal in custom folder and log paths and stopped CDN provider credentials appearing in administrator request URLs. Update to Cache Cleaner 10.0.0.

GeoIP and Conditions: spoofable IP headers

GeoIP fixed something that reaches every site using it for access control: **GeoIP lookups trusted spoofable forwarded client-IP headers**. If you gate content, logins or Regular Labs Conditions on a visitor's country or IP, an attacker could forge the header and present as any location they liked. The same spoofing fix appears in the Conditions component that ships with Advanced Module Manager, Conditional Content, Content Templater and ReReplacer, so it is not only GeoIP users who benefit. GeoIP's database-update path also fixed SSRF, credential exposure and unsafe archive extraction. Update GeoIP to 7.0.0 and the Conditions-bearing extensions to their fixed versions.

The "Anywhere" content plugins: SSRF and stored XSS

Articles Anywhere, Modules Anywhere and Users Anywhere render content through front-end tags, and all three fixed the same shape of problem. **External image downloads accepted unsafe hosts, redirects and local folders** (SSRF), **tag-provided custom HTML could render unsafe markup** (stored XSS), and tags could **expose restricted or unpublished content and authentication data**. Several of the fixes are breaking changes: tag-provided custom HTML now renders as escaped text rather than markup, so if you relied on that behaviour, test after updating. Update Articles Anywhere to 19.0.0, Modules Anywhere to 9.0.0 and Users Anywhere to 2.0.0.

Sourcerer tightens who can run PHP

Sourcerer lets you place code, including PHP, inside Joomla content, which makes it powerful and sensitive in equal measure. Version 13.0.0 **restricts PHP in articles to content created and last modified by Super Users**, and enforces the configured CSS, JavaScript and PHP permissions across both the creator and the last editor of an article, closing the gap where a lower-privilege editor could get code executed. This is separate from the older Sourcerer code-execution issue CVE-2025-22204, fixed back in 11.0.0. Note that 13.0.0 keeps your existing Pro security settings on update, so open the configuration and opt into the stricter defaults on purpose.

These are extension flaws, not a Joomla core problem

The distinction is worth getting right, because the Joomla community rightly bristles when extension issues get reported as “Joomla vulnerabilities”. Nothing in this release is a flaw in Joomla itself. Joomla core is unaffected. What happened is that a single vendor whose code is installed almost everywhere shipped fixes across its whole range at once, which is a different thing from a core security release.

It also changes how you respond. You do not need to touch Joomla core for any of this. You need to update the Regular Labs extensions, and you need to know which of your sites run them, because the blast radius here is defined by “do you have this extension installed”, not by your Joomla version.

No CVE does not mean no risk

There are no CVE numbers on the 22 July issues, and it would be easy to read that as “not serious”. That inference is wrong. A CVE is a tracking identifier, not a severity rating, and plenty of dangerous issues never get one, especially when a vendor fixes them in a changelog rather than filing an advisory. An unauthenticated SSRF or a stored XSS is exactly as exploitable whether or not a number is attached to it.

No CVE today also does not mean no CVE ever. To be clear, these are not our findings. We did not report them, and we do not know whether anyone has requested CVE numbers for them. This was Regular Labs’ own security pass across its codebase, fixed and shipped by the vendor. Numbers may still be assigned weeks or months from now, once a researcher or the Joomla CNA works through the changelog, so treat a missing CVE as paperwork that has not caught up rather than a verdict on severity.

What the missing CVE does change is your ability to hear about it. Without an advisory, an NVD entry or a Vulnerable Extensions List row, the only signal is a `[SECURITY FIX]` line in a per-extension changelog you have to go and read. That is the gap a live inventory closes: you find out because your dashboard tells you a version is outdated, not because you happened to be reading Regular Labs’ release notes on the right day.

How do I find every affected site I manage?

For up to about ten sites, log in to each Joomla administrator and check the installed Regular Labs versions against the fixed numbers above. Past that, checking by hand stops being realistic, and the risk is not the sites you remember but the ones you forget.

mySites.guru keeps a live inventory of every extension, template and framework on every connected Joomla and WordPress site in your account. Search for a Regular Labs extension once and you get every site running it, the version each is on, and whether an update is available. Because we have added detection rules for the affected versions, the vulnerable installs are already flagged for you, so you are working from a list rather than a search.

How do I update Regular Labs extensions safely?

1. **Take a backup first.** Before any extension update on a production Joomla site, back up the database and files. With mySites.guru you can trigger a snapshot or a full backup first.
2. **Update through Joomla's Extensions manager, or in bulk.** On a single site, open the Joomla administrator, go to System, then Update, then Extensions. If you manage many sites, use the mySites.guru mass update feature to upgrade every affected site from one dashboard.
3. **Mind the PHP 8.2 floor.** This release raises the minimum PHP version to 8.2 across the catalogue. Sites still on PHP 8.1, which reached end of life in December 2025, or older will not be offered the update until PHP is upgraded, which leaves them stuck on the vulnerable builds and is its own reason to move off an unsupported PHP version.
4. **Confirm the version and test.** After updating, check each extension reports the fixed version. Several fixes are breaking changes, especially in the Anywhere plugins where tag HTML now renders escaped, so test any site that relies on that behaviour.
5. **Do not rely on auto-updates blindly.** If you use Joomla extension auto-updates, confirm each site actually received the fix. Auto-updates fail more often than people think.

A coordinated hardening pass is a good sign, not a bad one

It can look alarming when a vendor patches its entire catalogue on one day. Read the other way, it is what responsible maintenance looks like. Regular Labs clearly ran a security pass across its whole codebase, found a class of issues, and fixed them everywhere at once rather than one reactive patch at a time. That is the same healthy pattern we see when we are not the only ones auditing Joomla extensions: the extensions getting this attention are the well-maintained ones.

None of this is a reason to distrust Regular Labs. The real takeaway is that keeping extensions updated is security-critical work, not cosmetic housekeeping, and "I would have updated if I had known" is not a plan when the disclosure is a changelog line on one of thirty extensions. Knowing which of your sites are affected, the day the fix ships, is the whole game. That is the job mySites.guru does for you.

Get free email alerts when a Joomla vulnerability breaks

We email a plain-English alert the moment a serious Joomla extension flaw is disclosed, with the affected versions and what to do. No charge, unsubscribe any time.

Subscribe to security alerts

Want the alerts and the tooling to act on them? Start with a free audit on one site and see your full extension inventory, or sign up for mySites.guru to get vulnerability alerts and one-click updates across every site you manage.

Timeline

2026-07-22 — **Roughly 30 extensions are updated at once**

A coordinated security-hardening release across the Regular Labs catalogue, which the vendor says runs on more than 100,000 websites.

The shared Regular Labs Library alone sits on more than 16,000 of the Joomla sites we manage.

2026-07-22 ● **Two of the fixes are in the shared Library, so they touch every extension**

Privileged AJAX endpoints that did not consistently enforce tokens and permissions, and a bundled HTTP-message library updated to close a request start-line injection. Cache Cleaner had the most serious set of its own: server-side request forgery reaching private networks, and OS command injection.

2026-07-22 ○ **No CVE numbers, which is not the same as not serious**

A CVE is a tracking identifier, not a severity rating. Plenty of genuinely dangerous issues never get one, especially when a vendor fixes them in a changelog rather than filing an advisory.

2026-08-17 ○ **Sourcerer needs three more releases of its own**

A separate flaw in one of the same catalogue's extensions, CVE-2026-74253, took 14.0.0, 15.0.0 and finally 16.0.0 on 26 August to close, and was exploited in the wild throughout. Being patched on 22 July does not help with that one.

Further Reading

- Regular Labs latest releases - the per-extension changelogs for the 22 July 2026 release, with every `[SECURITY FIX]` line.
- Why AJAX endpoints are a CMS security blind spot - the recurring public-endpoint pattern behind the catalogue-wide AJAX fix.
- A month of Joomla security disclosures - the wider run of Joomla extension issues this sits alongside.
- The Joomla and WordPress vulnerable extension list - how mySites.guru tracks known-vulnerable versions across your sites.

- CWE-918: Server-Side Request Forgery and CWE-79: Cross-Site Scripting - the canonical references for the two most notable weakness classes in this release.

Frequently Asked Questions

What did Regular Labs release on 22 July 2026?

Regular Labs shipped a coordinated security-hardening update across roughly 30 of its Joomla extensions on the same day, including Advanced Module Manager, Articles Anywhere, Cache Cleaner, GeoIP, Sourcerer, Modals, Tooltips, Keyboard Shortcuts and Modules Anywhere. Two of the fixes appear in every extension because they live in the shared Regular Labs Library: privileged AJAX endpoints that did not consistently enforce tokens and permissions, and a bundled HTTP-message library updated to close a request start-line injection. Individual extensions also fixed their own issues, from server-side request forgery to stored cross-site scripting. No CVEs were assigned.

Are these Joomla core vulnerabilities?

No. Every issue in this release is in a Regular Labs extension, not in Joomla itself. Joomla core is unaffected. The confusion is common because Regular Labs extensions are so widely installed, but the fix is to update the extensions, not Joomla.

Which Regular Labs extension issues are the most serious?

Cache Cleaner stands out: it fixed a server-side request forgery to private networks, an OS command injection where a request host value could reach a shell command on SiteGround hosts, path traversal and credential exposure. GeoIP fixed unauthenticated client-IP header spoofing that can bypass GeoIP-based access rules. The Articles, Modules and Users Anywhere content plugins fixed SSRF via external image downloads, stored XSS through unsafe tag HTML, and exposure of restricted content and authentication data. Sourcerer 13.0.0 restricts PHP in articles to Super Users.

Were any CVEs assigned to this Regular Labs release?

No CVE numbers were assigned to the 22 July 2026 issues at the time of writing. These were not reported by mySites.guru, so we cannot say whether anyone has requested CVEs, and numbers could still be assigned later. The vendor documented the fixes only in the per-extension changelogs, tagged [SECURITY FIX], rather than publishing a separate advisory. The exception is Sourcerer, which had an older, separate code-execution issue (CVE-2025-22204) fixed in 11.0.0; the 13.0.0 hardening is additional.

How do I find every Regular Labs extension across the Joomla sites I manage?

Up to about ten sites you can log in to each Joomla administrator and check the installed versions by hand. Past that, mySites.guru keeps a live inventory of every extension on every

connected Joomla and WordPress site. Search for the extension once and get back every site running it, the version each is on, and whether an update is available. mySites.guru has already added detection rules for the affected versions, so vulnerable installs are flagged automatically.

Do I need to worry if my sites already auto-update extensions?

If Joomla extension auto-updates are enabled and working, the fixed versions will install on their own, but you should still confirm each site actually received them. Auto-updates fail silently more often than people expect, usually because of a Download Key problem or a failed update site. mySites.guru shows you which sites are genuinely on the fixed version rather than which ones should be.

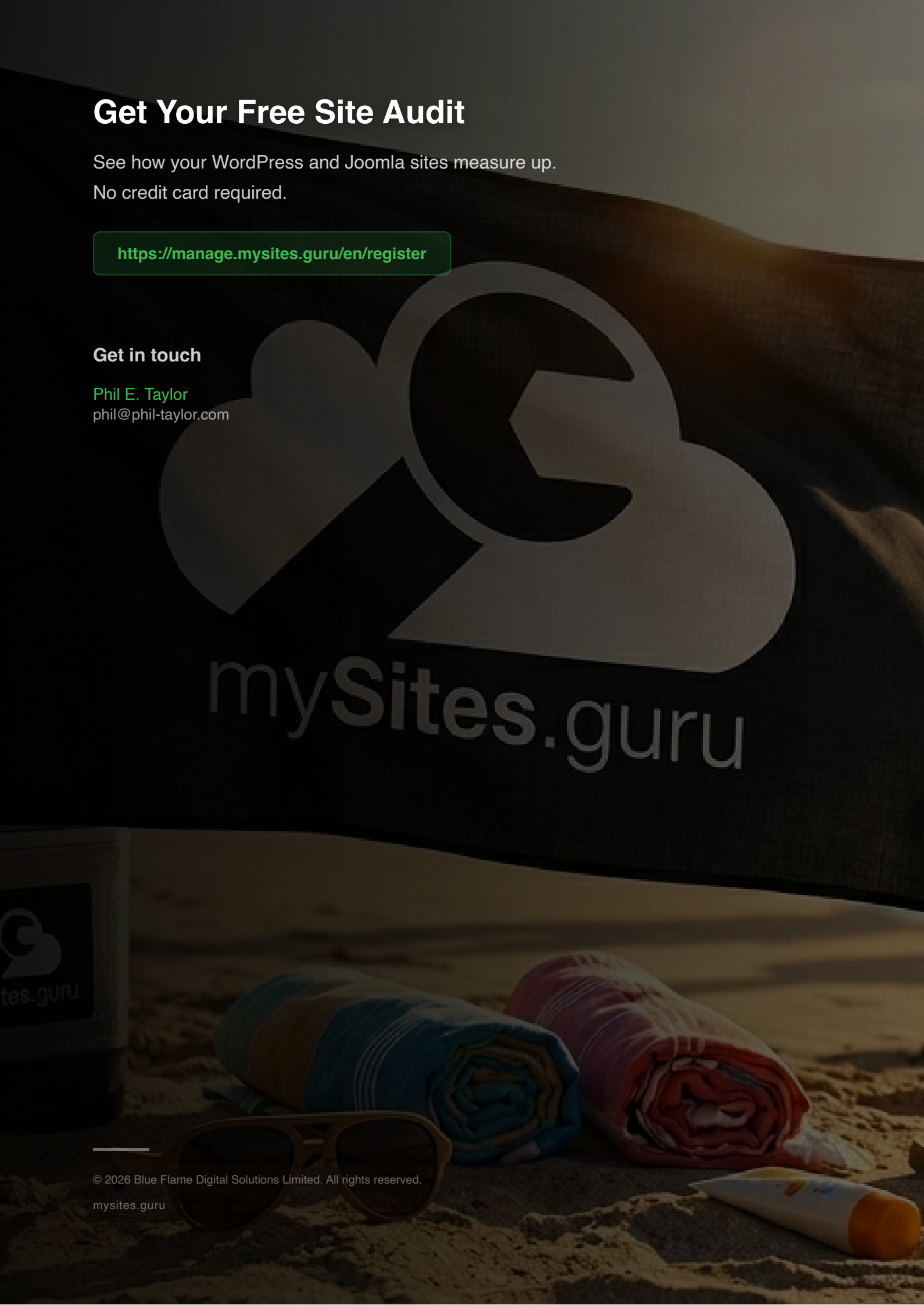
Written and edited by a human, with AI assistance. Our approach to AI

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

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.