mySites.guru

Regular Labs Publishes 24 Joomla Extension Updates Including 10 Security Fixes

Regular Labs shipped 24 Joomla extension updates on 13 September 2026. Ten fix security issues across nine CVEs, and four change behaviour on update.

Phil E. Taylor | 13 September 2026

Regular Labs, Peter van Westen's Joomla extension house, published 24 extension updates on 13 September 2026. Every one of them shipped the same day. Ten have a `[SECURITY FIX]` entry in the changelog, covering nine CVE identifiers between them, and four of those ten are flagged by the vendor as `BC BREAK`.

This is the second catalogue-wide release in eight weeks. The 22 July round patched around thirty extensions with no CVE numbers attached at the time. Every version this batch marks as affected is a build from that July release or later, so the sites that did the right thing in July are precisely the sites with something to do again now.

> **Do Conditional Content first**
>
> CVE-2026-85192, fixed in Conditional Content 8.0.0, let an untrusted article author run PHP through an inline Condition Rule. That is code execution reachable by the lowest content-authoring role on a Joomla site. Everything else in this batch is cross-site scripting or information disclosure. If you triage nothing else, triage this one. It affects the Pro edition.

TL;DR

- **24 extensions updated**, all dated 13 September 2026. Ten have security fixes, fourteen are ordinary maintenance.
- **Nine CVE identifiers**, all still RESERVED and unpublished on release day, so no vulnerability database or scanner can show them yet.
- **Two CVEs span multiple extensions** because the code is shared. CVE-2026-85188 covers four extensions, CVE-2026-85196 covers two.
- CVE-2026-85192 **is the outlier**: PHP execution by an article author, in Conditional Content. The rest are XSS and information disclosure.
- **Four releases are flagged** `BC BREAK` and will stop working features until an administrator re-authorises them. This is a release to stage, not to push.

- **Every rule is already live in our vulnerability database**, so connected Joomla sites running an affected build are flagged now rather than whenever the CVE records publish.

What Regular Labs shipped on 13 September

All 24 releases, with the ten security ones marked. Version numbers link to the vendor's changelog entry.

Extension	Version	Security fix
Advanced Module Manager	12.1.0	Yes
Articles Anywhere	20.0.0	Yes, BC BREAK
Articles Field	5.0.5	
Better Frontend Link	2.2.11	
Cache Cleaner	10.0.7	
CDN for Joomla!	8.0.4	
Conditional Content	8.0.0	Yes, BC BREAK
Content Templater	14.2.0	Yes
DB Replacer	9.1.0	
Email Protector	6.3.12	
Extension Manager	9.3.5	
GeoIP	7.0.4	
IP Login	7.0.4	
Keyboard Shortcuts	4.0.4	
Modals	17.0.0	Yes, BC BREAK

Extension	Version	Security fix
Modules Anywhere	9.0.5	
Quick Index	5.0.5	Yes
ReReplacer	16.2.0	Yes
Snippets	11.0.0	Yes, BC BREAK
Sourcerer	16.0.2	
Tabs & Accordions	3.1.0	Yes
Tooltips	10.1.0	
Users Anywhere	2.1.0	Yes
What? Nothing!	19.79.4	

Two of the fourteen non-security releases still change security-relevant behaviour without the vendor labelling them as fixes. Cache Cleaner 10.0.7 “tightens destination checks for URLs requested after cache cleaning”, and Tooltips 10.1.0 adds the same author-group gate on JavaScript Events that earned Modals and Articles Anywhere a CVE. Neither is tagged, so neither gets a rule from us, but both are worth knowing about.

The ten security fixes

Nine CVEs, ten extensions. The affected range in every case starts at the July 2026 build and ends at the version below.

CVE	Extension	Fixed in	Issue
CVE-2026-85192	Conditional Content	8.0.0	Untrusted article authors could run PHP through inline Condition Rules

CVE	Extension	Fixed in	Issue
CVE-2026-85195	Articles Anywhere	20.0.0	JavaScript Events attachable by any content author
CVE-2026-85196	Articles Anywhere, Users Anywhere	20.0.0, 2.1.0	Request input unescaped, raw output open to any author
CVE-2026-85189	Modals	17.0.0	Modal links accepted `javascript:` URLs
CVE-2026-88853	Modals	17.0.0	JavaScript Events attachable by any content author
CVE-2026-88852	Snippets	11.0.0	Snippet variable overrides settable by any author
CVE-2026-85190	Quick Index	5.0.5	Crafted index class options allowed JavaScript injection
CVE-2026-85191	Tabs & Accordions	3.1.0	Crafted `data-rlta-alias` attributes ran JavaScript on click
CVE-2026-85188	Advanced Module Manager, Conditional Content, Content Templater, ReReplacer	12.1.0, 8.0.0, 14.2.0, 16.2.0	Condition Set labels could reference unrelated database fields

The shared-code pattern is the thing to take away. CVE-2026-85188 is one defect in one Condition Set implementation that ships inside four separate products, so patching Content Templater and stopping there leaves the same bug live in three other places. Regular Labs has always built this way, and it is why a catalogue-wide release is the normal shape of a fix here rather than an overreaction.

Every one of these needs an authenticated account with content rights. None is reachable by an anonymous visitor. That is the honest framing, and it is also why Conditional Content stands out: on a Joomla site the Author role is the lowest content role there is, and plenty of sites hand it out freely or allow self-registration into it.

Four of these releases will change how your site behaves

This is the part that matters operationally, and it is the part a CVE list will not tell you.

Articles Anywhere 20.0.0, Conditional Content 8.0.0, Modals 17.0.0 and Snippets 11.0.0 are all flagged `BC BREAK` by the vendor. In each case the fix was not to sanitise a value but to withdraw a capability that had been open to any content author and put it behind an author-group setting that starts switched off.

- **Articles Anywhere and Modals** now restrict JavaScript Events to selected article author groups by default.
- **Snippets** now restricts Snippet variable overrides the same way.
- **Conditional Content** now prevents untrusted article authors running PHP in inline Condition Rules.

In each case the new setting defaults to **Super Users only**. We confirmed that in the shipped packages rather than inferring it: the `javascript_events_usergroups` field in Articles Anywhere 20.0.0's plugin manifest sets `default="Super Users"`, and the code default matches. Articles Anywhere 19.0.6 has no such field and no gate at all, so this arrived whole in 20.0.0.

That default is the right one for a security fix, and it is also why sites will change behaviour. If a site legitimately uses any of those features from a non-Super-User account, and many do, the feature stops working the moment the update is applied, and keeps not working until an administrator re-authorises the groups that should have it. Nothing warns you. The page just renders without the behaviour it had yesterday.

The gate is also narrower than a group check alone. Regular Labs' shared security code only allows executable attributes through when the content is being rendered as a Joomla article, category or featured view, when the tag is actually present in the stored article row, and when the article's last editor is in an allowed group. Modules, templates and third-party components never qualify, whatever the group setting says. Anyone using these tags inside a module should expect them to stop working regardless of how the permission is configured.

Conditional Content is the gentlest of the four, and its own field description says so: existing saved Condition Sets keep working, and only the restriction on *saving* new PHP is enforced. The other three take effect on render.

> **Stage this batch before rolling it out**
>
> A security release that removes a working capability on purpose is a different risk profile from one that patches a string behind the scenes. Update a representative site first, check any page using JavaScript Events, Snippet variables or PHP Condition Rules, re-authorise the author groups you actually trust, and only then push the wave.

For what it is worth, the restriction is the correct call. Joomla's own default text filters put Author, Editor and Publisher on the Default Forbidden List, which strips `script` along with `iframe`, `object` and `embed`. Only Super Users get unfiltered HTML, and core tightened this on purpose in 3.8.8 so that even Administrators no longer get unfiltered content by default. An extension that let an Author put executable script in a page was not offering an expected capability. It was routing around a filter Joomla puts in front of that group on purpose.

Why no vulnerability scanner can see these yet

All nine CVE identifiers were still in RESERVED state on the day of release. The numbers are allocated, and Regular Labs has printed them in its own changelogs, but the records are not live at cve.org or in NVD. We checked the MITRE record endpoint, the NVD API and the CVE Project's own git mirror, and all three come back empty.

Everything downstream mirrors published records. That means the aggregators, the feeds, and most commercial scanners cannot show you a single one of these today. If your tooling is quiet on Regular Labs this week, that silence is a gap in the data rather than a clean bill of health.

This is the same gap the July round sat in for weeks, and those numbers did eventually arrive. One of them, the Sourcerer issue, turned out to need a second fix release once

it was properly scored.

We do not wait for publication. All 34 matching rules for this batch went into our Joomla vulnerability database on release day, so every connected site running an affected build is already flagged with the version that resolves it.

Regular Labs did announce the release publicly and did so promptly, posting eleven times on Mastodon within twelve minutes of the packages going live, each post linking its own changelog. The problem is reach rather than intent. That account had around 70 followers when we checked, the vendor's RSS feed has not had an item since 2019, there is no security page and no mailing list signup anywhere on the site. The summary post announcing all 24 updates does not use the word security at all, and the Modals post hit Mastodon's character limit mid-sentence, so one of the two CVE numbers for that extension is simply not in it.

None of that is concealment. It is a release that was announced into a room with almost no one in it, while the CVE records that would have spread it further sat unpublished. If you maintain Joomla sites and you learned about this from us rather than from the vendor, that is why.

What the sites we monitor actually look like

We can see the installed version of every Regular Labs extension across the Joomla sites connected to mySites.guru. Measured on release day, across the ten affected extensions, the picture splits in a way that is worth sitting with.

62.8%
on the July build
current until this morning, newly affected today

36.7%
already behind
running a version with a published CVE before today

0.5%
already patched

as expected on release day

Share of installs across the ten affected extensions, on Joomla sites snapshotted in the last 30 days.

The 62.8% is unremarkable. Those sites were fully current when they went to bed and are affected because a new release exists, which is how patching works.

The 36.7% is the number worth acting on, and when we broke it down by the age of the installed build it turned out not to mean what we first assumed.

Around 32% of all installs we monitor sit on a build dated 4 September 2023 or earlier, with almost nothing in between that and the current release. The obvious reading is a large group of abandoned sites. The obvious reading is wrong.

The 2023 cluster is Joomla 3, and it is stranded rather than neglected

4 September 2023 is the date Regular Labs last shipped a build for Joomla 3. Pull the vendor's own update feed and every Joomla 3 branch is frozen on that day: Articles Anywhere at 14.2.0, Modals at 12.6.1, Snippets at 8.7.0, Quick Index at 3.6.0, Content Templater at 11.5.0, ReReplacer at 13.2.0. The Joomla 4, 5 and 6 branch is versioned separately and is the only one receiving this batch.

Those terminal version numbers are exactly the versions clustering in our data. Measured across the seven affected extensions with a Joomla 3 branch, 19.1% of installs are sitting on precisely the last build Regular Labs ever released for their platform, and a further 11.8% are older still.

That reframes the number. A fifth of these installs belong to sites that applied every update offered to them and then ran out of updates. Joomla's own update check tells them they are current, because as far as their branch is concerned they are.

None of these nine fixes will reach a Joomla 3 site

There is no Joomla 3 backport in this batch and there will not be one. For a site in that group the remediation is a migration rather than an update. Applying the fix means moving the site to Joomla 4 or later first, which is work of a completely different size, and worth scoping now rather than at the next release.

So the useful question after this release goes past whether you applied it: which sites in your portfolio could not receive it, and did you know which ones those were before today? The oldest Articles Anywhere install still connected to us is version 1.9.3, released in January 2011.

The vendor's own update feed is still behind its own release

One practical wrinkle, checked at 16:17 UTC on release day, roughly three hours after the packages went live.

Joomla sites do not poll the changelog page. They poll `download.regularlabs.com/updates.xml`, and that feed was still offering the previous version for three of the ten affected extensions: Quick Index at 5.0.4, Content Templater at 14.1.0 and Users Anywhere at 2.0.6. Articles Anywhere and Snippets had already rolled over, and Snippets flipped while we were watching, so this is staggered propagation rather than a broken feed. The feed sets a six hour cache lifetime, which fits.

It still means a site checking for updates this afternoon may be told it is current on three extensions that are not. If you are working through this batch today and an extension reports nothing available, check the version against the table above rather than trusting the prompt.

How do you update 24 extensions safely?

1. **Take a backup first.** Four of these releases change behaviour on purpose, so a rollback path is not optional this time.
2. **Do Conditional Content first** if you run it. CVE-2026-85192 is the only code execution issue in the batch.
3. **Update one representative site**, then open a page that uses JavaScript Events, Snippet variables or PHP Condition Rules and confirm it still does what it should.
4. **Re-authorise the author groups** you actually trust in each of the four BC BREAK extensions, rather than disabling the new restriction wholesale. The restriction is the fix.
5. **Check your template overrides.** Articles Anywhere 20.0.0 also changes full article layouts in feeds, which is exactly where a stale override bites.
6. **Do not trust an empty update prompt today.** The vendor's update feed was still serving the previous version for three of the ten extensions three hours after release. Check the installed version against the table above.
7. **Separate out your Joomla 3 sites.** They cannot receive any of this. Put them on a migration list rather than an update list.
8. **Then roll the wave**, and turn on automatic updates for the extensions where you are comfortable with it, so the next catalogue-wide release is not another manual afternoon.

How do I find every site running a Regular Labs extension?

Checking 24 extensions by hand across a portfolio is the kind of job that gets postponed, which is how a site ends up on a 2023 build.

mySites.guru keeps an extension inventory for every connected Joomla site. Searching the extension inventory for any of these names returns every install and its version on one screen, and anything below the fixed version is flagged automatically against the rules we added on release day. You get a list of sites to fix rather than a list of sites to check.

The official Joomla Vulnerable Extensions List will almost certainly not record this release, and the public CVE databases cannot yet. That gap between what a vendor has fixed and what the world can see is the whole reason we keep our own vulnerability database rather than mirroring someone else's.

Timeline

4 September 2023

The last Joomla 3 build

Regular Labs shipped its final Joomla 3 release across the range on this date. Every Joomla 3 branch in the vendor's update feed is still frozen here, which is why a fifth of the installs we monitor sit on exactly these version numbers.

22 July 2026

The catalogue-wide security release

Around thirty extensions patched at once, with no CVE identifiers assigned at the time. Every version marked affected in today's batch is a build from that release or later.

17 August 2026

Sourcerer 16.0.0 closes CVE-2026-74253

The July round's Sourcerer fix turned out to be incomplete, and the issue was assigned a CVE retroactively. Evidence that a Regular Labs fix release can itself need re-scoping.

13 September 2026

Twenty four updates, ten with security fixes

Nine CVE identifiers across ten extensions, four of them flagged BC BREAK. All nine CVE records were still RESERVED and unpublished on the day of release.

Further Reading

- Regular Labs Patched Its Whole Joomla Extension Catalogue at Once - the 22 July 2026 round, and the source of every version number now marked affected
- Sourcerer 14 and 15 did not fix CVE-2026-74253. 16.0.0 does. - what happens when a Regular Labs fix release needs re-scoping
- Twenty Rules for Joomla Extension Developers Handling a Security Report - the yardstick we measure vendor handling against
- One VEL for Every Joomla and WordPress Site - why the official Vulnerable Extensions List will not record this release
- Automatic Updates for Any Joomla Extension - how to stop a twenty four extension wave being a manual job
- Regular Labs latest releases - the vendor's own changelog index, the only published source for this batch
- CWE-79: Improper Neutralization of Input During Web Page Generation - the class covering most of this batch

Frequently Asked Questions

What did Regular Labs release on 13 September 2026?

Twenty four Joomla extension updates, all on the same day. Ten of them have a [SECURITY FIX] entry in the changelog, covering nine CVE identifiers between them. The other fourteen are ordinary maintenance releases with bug fixes, translation updates and the removal of the automatic Download Key popup. Four of the ten security releases are also flagged by the vendor as BC BREAK, meaning they change behaviour that working sites may depend on, on purpose.

Which Regular Labs extensions have security fixes?

Ten: Advanced Module Manager 12.1.0, Articles Anywhere 20.0.0, Conditional Content 8.0.0, Content Templater 14.2.0, Modals 17.0.0, Quick Index 5.0.5, ReReplacer 16.2.0, Snippets 11.0.0, Tabs and Accordions 3.1.0, and Users Anywhere 2.1.0. Two of the nine CVEs span more than one extension because the affected code is shared: CVE-2026-85188 covers four extensions and CVE-2026-85196 covers two.

Which is the most serious issue in this batch?

CVE-2026-85192 in Conditional Content, fixed in 8.0.0. Before that release an untrusted article author could run PHP through an inline Condition Rule. That is arbitrary code execution reachable by the lowest content-authoring role on a Joomla site, and on any site that lets people register with authoring rights an attacker can create that account themselves. The other eight issues are cross-site scripting or information disclosure.

Why can't I find these CVEs in any vulnerability database?

Because all nine are still RESERVED rather than published. The identifiers are allocated and Regular Labs has printed them in its own changelogs, but the records themselves are not live at cve.org or NVD yet, so nothing that mirrors published CVE data can show them. That includes most commercial scanners. A quiet scanner right now is not evidence that your sites are fine.

Will updating break my site?

It can, and on four of these releases it is meant to. Articles Anywhere 20.0.0, Conditional Content 8.0.0, Modals 17.0.0 and Snippets 11.0.0 all restrict a capability that used to be open to any content author. If your site legitimately uses JavaScript Events, Snippet variable overrides or PHP in Condition Rules, those will stop working after the update until an

administrator re-authorises the author groups allowed to use them. Test on a staging copy before rolling the update across a portfolio.

I still run Joomla 3. Do I get these fixes?

No, and there will not be a backport. Regular Labs stopped shipping Joomla 3 builds on 4 September 2023, and every Joomla 3 branch in the vendor's update feed is still frozen on that date: Articles Anywhere 14.2.0, Modals 12.6.1, Snippets 8.7.0, Quick Index 3.6.0, Content Templater 11.5.0, ReReplacer 13.2.0. Your site will report itself as up to date because it is, for its branch. Roughly a fifth of the installs we monitor are sitting on exactly those terminal versions. For those sites the remediation is migrating off Joomla 3, not applying an update.

How do I find every site running a Regular Labs extension?

By hand you would log into each Joomla site and read its extension list, which is slow enough that it gets skipped. mySites.guru keeps an extension inventory for every connected site, so searching for an extension name returns every install with its version on one screen, and any site below the fixed version is flagged automatically with the version that resolves it.

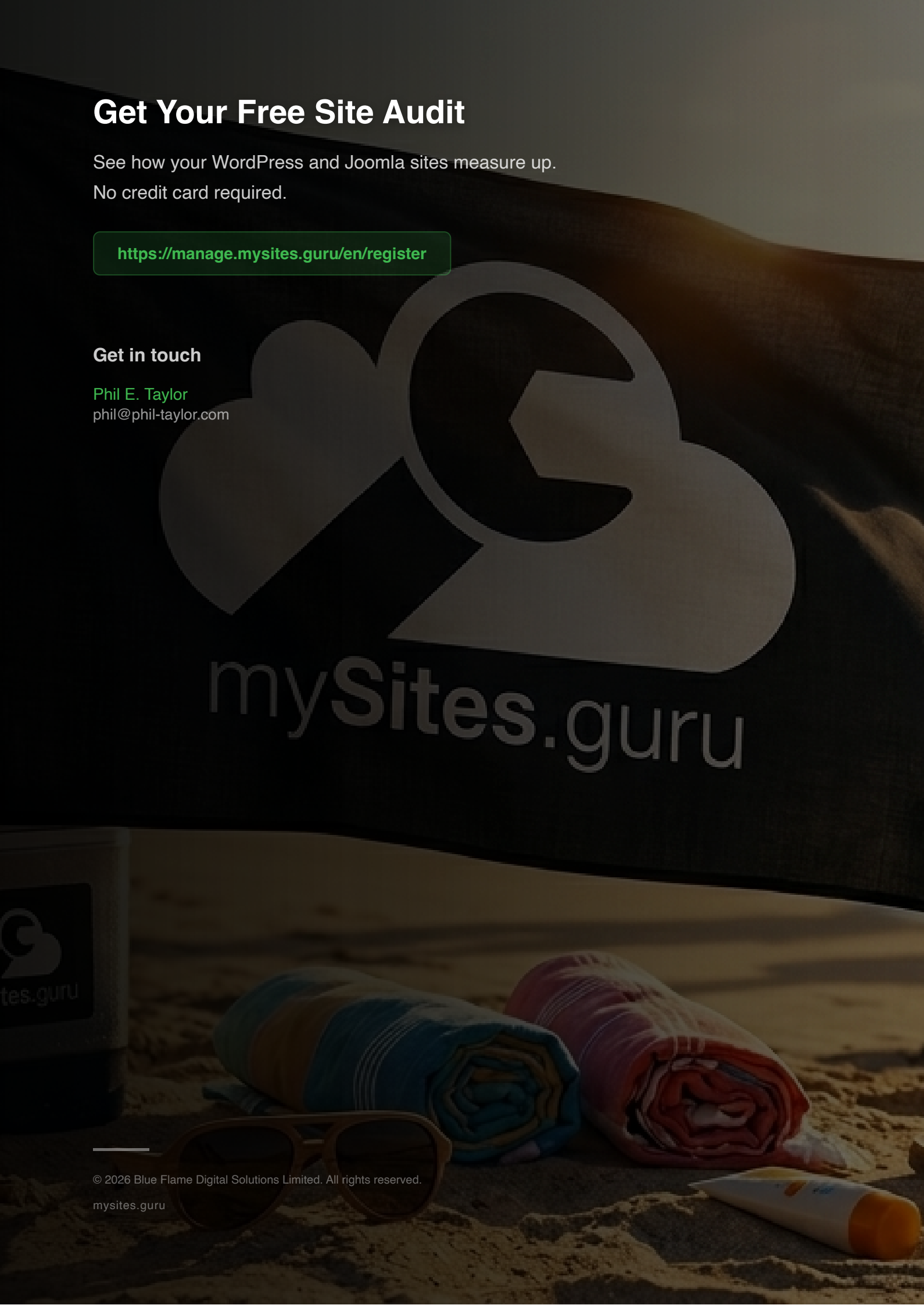
Written and edited by a human, with AI assistance. Our approach to AI

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