mySites.guru

AcyMailing Vulnerability Also Affects Joomla Sites

CVE-2026-3614 is listed as a WordPress bug. We diffed the 10.8.1 and 10.8.2 source and the same vulnerable code ships to Joomla sites too.

Phil E. Taylor | 16 April 2026

Yet again, a vulnerability in a dual WordPress/Joomla plugin only gets noticed and shouted about in WordPress circles, leaving Joomla users blind and none the wiser.

This time it is AcyMailing, a newsletter plugin with a Joomla component and a WordPress plugin built from the same source tree. CVE-2026-3614 is a CVSS 8.8 privilege escalation, and every advisory we could find describes it as WordPress-only. None of them mention Joomla.

We downloaded the Joomla installer tarballs for AcyMailing 10.8.1 and 10.8.2, ran a diff, and found the patch sitting in shared code that ships to Joomla sites too. The AcyMailing vendor changelog also confirms it: the 10.8.2 security entry is flagged with both the Joomla and WordPress icons, so the vendor themselves are telling you both platforms are affected - the CVE just doesn't. If your Joomla site runs AcyMailing 9.11.0 through 10.8.1, your attack surface is identical to the WordPress sites the CVE was written for.

Hundreds of Joomla and WordPress sites connected to mySites.guru are running an affected version right now. Here is what the bug actually does, why the public record missed Joomla, and what to do about it.

TL;DR

- CVE-2026-3614 — CVSS 8.8 privilege escalation in AcyMailing 9.11.0 through 10.8.1
- Public CVE describes it as a WordPress-only bug. **It is not.** Joomla is equally affected
- Patch shipped in **AcyMailing 10.8.2** on 13 March 2026. Update every Joomla and WordPress site running it
- Vendor changelog flags the fix with both the Joomla and WordPress icons. Our own source diff proves the vulnerable code is in shared `back/Core/AcymController.php`

- Joomla's Vulnerable Extensions List has no entry for this CVE. The most recent VEL entry is from February 2026

This is the second recent case of a cross-platform plugin vulnerability being disclosed for WordPress only while Joomla site operators receive no public warning. Smart Slider 3 (CVE-2026-3098) was the previous one. The pattern is becoming familiar.

How to Check Your Sites for AcyMailing 9.11.0 to 10.8.1 with mySites.guru

When a privilege escalation CVE drops in a plugin that ships on both Joomla and WordPress, the first question every agency asks is: "Which of my sites are running a vulnerable version?" If you manage 50 or 200 client sites across both CMS platforms, logging into each admin panel and checking the AcyMailing version is not viable. By the time you get through the list, the attacker has already had their month of diff-and-exploit lead time.

mySites.guru's twice-daily extension snapshot records the exact version of every installed plugin and Joomla extension across every connected site. The extension search page lets you filter by version number in seconds.

If you are already a mySites.guru subscriber, the AcyMailing extension search page lists every installed version across all your connected Joomla and WordPress sites, grouped by version number. Filter for anything between 9.11.0 and 10.8.1 to see which sites need the update.

View all your AcyMailing installations

Open AcyMailing Extension Search

Lists every installed version across all your connected Joomla and WordPress sites. Filter by 9.11.0 through 10.8.1 to find vulnerable installations that need to move to 10.8.2.

Combined with the mass plugin updater, you can push 10.8.2 across every affected site in one batch. A cross-platform CVE becomes a five-minute triage instead of a full day of logging into client admin panels.

If you do not have a mySites.guru account yet, start a free trial and connect your sites. The plugin index builds automatically on the first snapshot.

Checking manually without mySites.guru is a lot of work with a lot of sites

If you manage sites outside of mySites.guru, log into each admin and check the version:

- **Joomla:** open **Components → AcyMailing → Configuration**. The version number is at the bottom of the page.
- **WordPress:** open **Plugins → Installed Plugins** and look at the AcyMailing row.

Anything 9.11.0 through 10.8.1 needs updating. The AcyMailing changelog lists the latest release, and the download comes through your AcyMailing account.

How does mySites.guru help subscribers when a vulnerability is found?

Finding the affected sites is the easy bit. Once you know which ones are vulnerable you still have to triage, patch, verify, and sometimes clean up after exploitation. Here is how mySites.guru handles each stage.

Twice-daily extension snapshots

Every connected Joomla and WordPress site is snapshotted twice a day. The snapshot records the plugin index, CMS core version, PHP version, server modules, and active templates. When a new CVE lands, the latest snapshot is at most 12 hours old, so you are not looking at yesterday's state. Cross-platform CVEs like this AcyMailing one show up across both CMS families in the same query.

Cross-referenced vulnerability alerts

Snapshot data gets matched against the Wordfence and Patchstack feeds automatically. Any WordPress CVE that also hits a Joomla-side plugin (because the plugin ships dual-platform from shared code) surfaces on the affected Joomla sites too. That closes the gap that caught this AcyMailing CVE out.

Alerts fire to email and appear on the dashboard the morning the feeds update. No polling, no manual cross-reference.

One-click bulk updates

Once vulnerable versions show up in your portfolio, the mass plugin updater pushes the fixed version to every affected site in one batch. Joomla and WordPress sites update through the same workflow. No logging into client admin panels one at a time.

Post-update verification audits

A full site audit runs after each update to verify the plugin is at the expected version and the site is still healthy. The audit catches updates that silently failed, sites that went down, and file-integrity checks that broke. You get a report rather than having to spot-check manually.

File-level malware scanning for post-exploitation

An update does not undo exploitation that already happened. mySites.guru's malware scanner runs file-level integrity checks and pattern matching for known backdoors and droppers, and the hacked-files detector walks through how to interpret the results. When Astroid Framework was being actively exploited in March 2026, the scanner flagged the BLPayload droppers on customer sites on the next audit cycle, before any public IoC list existed.

Changelog and incident dashboard

Every new CVE writeup, mass-exploitation wave, and plugin backdoor incident goes on the account changelog so subscribers have a running record of what happened, when, and what needed doing. The AcyMailing CVE-2026-3614 entry is there too.

For Joomla operators, this is the closest thing the ecosystem has to a commercial vulnerability pipeline. Imperfect, and dependent on the WordPress-side CVE feeds catching the bug first - but it is what exists until someone builds a Joomla-native equivalent.

What does the AcyMailing vulnerability actually do?

At CVSS 8.8 this is a privilege escalation, not remote code execution. An attacker needs an authenticated account on the target site. On WordPress that means a Subscriber-level user, the lowest privilege WordPress offers. On Joomla it means any registered user whose ACL grants them access to the relevant AcyMailing routes.

From that low-privilege starting point, the vulnerability lets the attacker call admin-only controller methods on the AcyMailing component. The public Wordfence-style writeup describes the attacker:

1. Turning on AcyMailing's autologin feature via the configuration controller
2. Creating a malicious newsletter subscriber with an injected `cms_id` pointing to any existing CMS user, including administrators
3. Using the autologin URL to authenticate as that user

You sign up as a subscriber, walk in as the admin. That is the whole chain.

Why does the AcyMailing CVE only mention WordPress?

Because Joomla has no commercial CVE reporting infrastructure, and WordPress does. That is the entire answer. Everything below is the detail.

WordPress has three separate commercial vulnerability research operations paying people to break their plugin ecosystem:

- Wordfence is a CVE Numbering Authority, so they can issue CVE IDs directly without going through MITRE. They also run the Wordfence Bug Bounty Program that pays researchers to report plugin vulnerabilities.
- Patchstack is also a CNA, runs the Patchstack Alliance bug bounty, and coordinates responsible disclosure with plugin authors.
- WPScan is owned by Automattic (the company behind WordPress.com) and maintains a vulnerability database that feeds commercial security plugins.

All three scan every WordPress plugin update looking for silent security fixes. All three pay staff to produce CVEs and advisories.

Joomla has a CNA too - the Joomla Security Strike Team became one in November 2020 - but their scope in practice is Joomla core, not third-party extensions. They rarely issue CVEs for extension bugs. Beyond that, there is nothing: no bug bounty, no commercial researcher community, no release scanning. The Joomla Vulnerable Extensions List is volunteer-run and reporter-led - somebody has to send them a report before an entry appears. On the day CVE-2026-3614 dropped, VEL's most recent entry was from 27 February 2026. No CVE-2026-3614 entry was added.

mySites.guru is as close as the Joomla world gets to the Wordfence/Patchstack role, and we are honest about the limits: we cross-reference extension versions on every connected site against the WordPress vulnerability feeds twice a day, which closes the gap on cross-platform plugins but is not a replacement for a funded Joomla CVE pipeline. Nothing is. Until someone decides to build a Joomla Wordfence and fund it, this asymmetry is going to keep happening. Joomla operators who only watch CVE feeds see the AcyMailing disclosure, see the word "WordPress", and move on. Their sites stay exposed.

How we proved CVE-2026-3614 affects Joomla AcyMailing too

AcyMailing's download API only serves the latest version, but acyba's GitHub organisation maintains tagged source for older releases. We pulled the 10.8.1 and 10.8.2 Joomla-compiled tarballs and ran `diff -rq` across the two trees.

The files that differ between the two releases are the ones the WordPress CVE writeup points to:

- `back/Core/AcymController.php`
- `back/Classes/UserClass.php`
- `back/Controllers/ConfigurationController.php`
- `front/FrontControllers/FrontconfigurationController.php`

These are not WordPress-specific files. They live under `back/` and `front/`, the platform-agnostic AcyMailing core. The `WpInit/` folder the public CVE writeup references is the WordPress integration layer that calls into this shared code.

How the authorization bypass works

In vulnerable versions of `back/Core/AcymController.php`, the authorization gate looks like this:

```
public function call(string $task): void
{
    // If not authorized, display message and redirect to dashboard
    if (!in_array($task, ['countResultsTotal', 'countGlobalBySegmentId', 'c
        && strpos($task, 'Ajax') === false
        && !acym_isAllowed($this->name)) {
        acym_enqueueMessage(acym_translation('ACYM_ACCESS_DENIED'), 'warnir
        acym_redirect(acym_completeLink('dashboard'));
    }
    // ... dispatch the task
}
```

The second condition is the bug. `strpos($task, 'Ajax') === false` means: **if the task name contains the word "Ajax", skip the authorization check entirely.** Any

controller method named `somethingAjax` can be called by any authenticated user, with no permission check at all.

In 10.8.2 the gate is three lines and every task goes through `acym_isAllowed()`:

```
public function call(string $task): void
{
    if (!acym_isAllowed($this->name)) {
        acym_enqueueMessage(acym_translation('ACYM_ACCESS_DENIED'), 'warnin
        acym_redirect(acym_completeLink('dashboard'));
    }
    // ... dispatch the task
}
```

How the subscriber injection works

`back/Classes/UserClass.php` is the second half of the chain. In vulnerable versions, the subscriber-save code does not strip `cms_id` or `key` from attacker-controlled input. That lets an attacker create a newsletter subscriber with:

- `cms_id` set to an administrator's user ID
- `key` set to a known autologin token

Combine that with the autologin feature toggled on (reachable via the AJAX controller bypass above), and the attacker can hit the autologin URL and authenticate as the admin.

In 10.8.2 both fields are stripped before save:

```
unset($user->cms_id);
unset($user->key);
```

This is the "user creation" fix the vendor's changelog refers to.

The vendor changelog confirms Joomla

This is the AcyMailing 10.8.2 changelog entry from acymailing.com:

> *"Vulnerability*
>
> *[Joomla icon] [WordPress icon] A vulnerability on user creation impacting versions 9.11.0 to 10.8.1 has been patched. Details will be disclosed after a reasonable time to let users apply the patch first."*

Both platform icons appear next to the vulnerability entry. The vendor confirms both CMS versions are affected. The public CVE does not.

AcyMailing is the sixth AJAX authorization CVE in eight weeks

We have been writing about this pattern for two months. CVE-2026-3614 is the sixth AJAX-authorization bug in that window, and the shape is the same every time. An AJAX endpoint authenticates the request (the user is logged in, the CSRF token is valid) but never checks whether the user is authorized to do the thing they're asking to do.

Eight weeks of CVE disclosures in Joomla and WordPress extensions:

- Astroid Framework (CVE-2026-21628) — CVSS 10.0, Joomla. AJAX endpoint checked the CSRF token but skipped the admin-authentication check. Grab the token from the login page, upload backdoors, done.
- Novarain Framework (CVE-2026-21627) — CVSS 9.5, Joomla. `com_ajax` endpoint with no authentication check, reachable via Convert Forms and EngageBox plugins.
- Smart Slider 3 (CVE-2026-3098) — WordPress. `admin-ajax.php` action with a valid CSRF check and no capability check. Any subscriber could download `wp-config.php`.
- **Joomla core (CVE-2026-21629)** — the Joomla Security Strike Team's own discovery that `com_ajax` was excluded from the default logged-in-user check in

the admin area. The framework routing every Joomla plugin's AJAX requests had the same authorization gap as the plugins built on top of it.

- Ninja Forms File Uploads (CVE-2026-0740) — CVSS 9.8, WordPress. Unauthenticated RCE via an `admin-ajax.php` handler that never checked anything.
- **AcyMailing (CVE-2026-3614, this post)** — CVSS 8.8, Joomla and WordPress. Internal AJAX router had a one-line `strpos($task, 'Ajax') === false` loophole that let any logged-in user reach admin-only controller methods.

Same root cause every time. A developer implemented CSRF protection (which stops requests originating on another domain) and assumed that covered access control (which decides who is allowed to do what). It doesn't. They defend against different threats and you need both.

Our March 2026 AJAX pattern post goes into why this keeps happening, what Joomla 5.4.4 did at the framework level for `com_ajax`, and why the official Joomla developer documentation still teaches the insecure pattern. AcyMailing fits the template. The vulnerable code called `acym_isAllowed()` on most tasks but had a `strpos('Ajax')` substring check that let any attacker slip past by picking an Ajax-suffixed task name. In 10.8.2 every task goes through the authorization function - which is what should have been happening since 9.11.0.

If you manage a portfolio of Joomla or WordPress sites with a pile of third-party extensions, assume this pattern is not done with us. More AJAX authorization CVEs are coming, probably this month. Patching each one as it lands is not a strategy - by the time the CVE is public the attackers have already had their month of diff-and-exploit time. What actually works is tracking extension versions across every site you manage and being able to pull up the list of vulnerable installs the same afternoon a CVE drops. That is the workflow mySites.guru is built around.

Why Joomla extensions keep getting left behind on CVE visibility

The gap is self-reinforcing. Fewer Joomla installations than WordPress means less commercial incentive to fund a Joomla-focused Wordfence. Less vulnerability research means fewer Joomla CVEs. Fewer CVEs makes Joomla look safer than it is, which kills urgency to build the missing infrastructure, which keeps the feedback loop going.

Meanwhile the WordPress side gets richer. Wordfence Premium sells firewall rules. Threat-intelligence subscriptions feed commercial products like Jetpack Scan, Sucuri, and Solid Security. Every new paying customer justifies more researcher hires. Every new CVE makes the feed more valuable. WordPress has turned plugin vulnerability disclosure into a funded commercial loop. Joomla has the Joomla Security Strike Team (core only) and VEL (volunteer-run, reactive).

When the vulnerability lives in cross-platform code, the asymmetry gets painful. Smart Slider 3 in March was the clearest recent case: the WordPress side got a CVE, a Wordfence advisory, coverage on every WordPress security blog. Joomla site operators found out via a German-language forum thread. Different plugin, same story here.

What to do right now about AcyMailing 10.8.2

If you only have a handful of sites: log into each Joomla admin, check the AcyMailing version, update to 10.8.2 via AcyMailing's Joomla installer.

If you manage tens or hundreds of sites: connect them to mySites.guru and the dashboard will show you every site running AcyMailing, the exact version, and flag the vulnerable range. The same screen pushes the 10.8.2 update to every affected site in one batch, for Joomla and WordPress together. This is the use case multi-site CMS management tools are built for.

If your extension auto-updates are disabled (Joomla disables them by default), you will have to push the update manually. Most AcyMailing installs we see across the portfolio are two or three minor versions behind. If the primary CMS you manage is Joomla, start watching the WordPress CVE feeds too - CVE-2026-3614 is proof that a WordPress-framed disclosure may hit Joomla anyway.

Was my Joomla site exploited via AcyMailing before I patched?

The vulnerability went public on 16 April 2026. The patch was available from 13 March 2026. So anyone with a GitHub account and 10 minutes of patience has had a month to diff the releases, work out the attack path, and quietly try it on whatever authenticated accounts they already had. If you are patching late, assume exploitation attempts happened.

Signs of compromise on a Joomla site:

- **New administrator accounts** you didn't create. Check **Users → Manage** and sort by registration date
- **AcyMailing configuration changes** you didn't make, specifically the autologin setting being turned on
- **New newsletter subscribers** with unusual `cms_id` values linking them to admin accounts
- **Autologin URLs in access logs** referencing AcyMailing routes with session-establishing tokens

If any of those turn up, assume the site is compromised and work through a Joomla hack recovery instead of just updating the plugin. Updating closes the door, but if an attacker already got in and established a secondary persistence mechanism (new admin, backdoor file, scheduled task), the update does not clean that up.

Further reading

- CVE-2026-3614 on Vulnerability-Lookup — the CIRCL CVE record with full technical metadata
- Managed-WP advisory — the most detailed public writeup of the WordPress attack path

- AcyMailing changelog — the vendor's own confirmation of the shared-code fix with both Joomla and WordPress icons
- acyba/acymailing on GitHub — tagged source for every public release, the diff we used is between `v10.8.1` and `v10.8.2`
- Joomla Vulnerable Extensions List and the VEL about page — the official statement of what VEL is and is not
- Wordfence vulnerability database, Patchstack database, and WPScan plugins directory — the three commercial WordPress vulnerability feeds CVE-2026-3614 appears in
- CVE Program list of CNAs — search for "Wordfence" and "Patchstack" to see the WordPress-focused CVE authorities; no Joomla equivalent exists
- OWASP Access Control Cheat Sheet — the distinction between authentication, authorization, and CSRF protection that plugin developers keep conflating

Stop missing Joomla CVEs that only get announced for WordPress

If Wordfence and NVD are the only feeds you watch, you will keep missing the Joomla half of cross-platform disclosures. Connect your sites to mySites.guru and the vulnerability scanner does the cross-referencing for both CMS platforms, twice a day. Every site running a vulnerable version, Joomla and WordPress together, in one list.

Frequently Asked Questions

Is CVE-2026-3614 only a WordPress vulnerability?

No. The public CVE record and every WordPress vulnerability database describe it as a WordPress-only issue. The AcyMailing vendor changelog for version 10.8.2 flags the same user-creation vulnerability with both the Joomla and WordPress icons, and a source diff of 10.8.1 against 10.8.2 shows the fix is in shared code that ships to both platforms. Joomla sites on AcyMailing 9.11.0 through 10.8.1 are affected.

Which AcyMailing versions for Joomla are vulnerable?

AcyMailing 9.11.0 through 10.8.1 inclusive. The patch ships in AcyMailing 10.8.2, released on 13 March 2026. Update the Joomla component immediately.

What is the actual vulnerability in the shared code?

In vulnerable versions of back/Core/AcymController.php, the authorization check bypasses any task name containing the string 'Ajax'. Any authenticated user, regardless of Joomla or WordPress privilege level, can call any controller method whose name matches the pattern and skip the acym_isAllowed() permission check entirely. The 10.8.2 release gates every task through acym_isAllowed() and applies strict task-name allowlisting on the clear() method.

Why does the public CVE only mention WordPress?

The vulnerability was reported via Wordfence, which is a CVE Numbering Authority and publishes advisories focused on WordPress plugins. Joomla has no equivalent funded vulnerability research pipeline. The Joomla Vulnerable Extensions List is volunteer-run and reporter-led, so vulnerabilities in shared Joomla and WordPress plugins routinely get documented only for the WordPress side.

How can I check if my Joomla sites are running a vulnerable AcyMailing version?

mySites.guru indexes every extension on every connected Joomla and WordPress site and cross-references versions. If you connect your sites, the dashboard shows every site running AcyMailing, the exact version, and whether that version is vulnerable. You can filter by AcyMailing 9.11.0 through 10.8.1 and push the update across your entire portfolio in one go.

Does this affect the free AcyMailing Starter edition for Joomla?

Yes. The vulnerable code is in back/Core/AcymController.php, which is part of the core component shared by the free Starter edition and every paid tier. All editions built from the same source tree are affected in the 9.11.0 to 10.8.1 range.

What should extension developers learn from this?

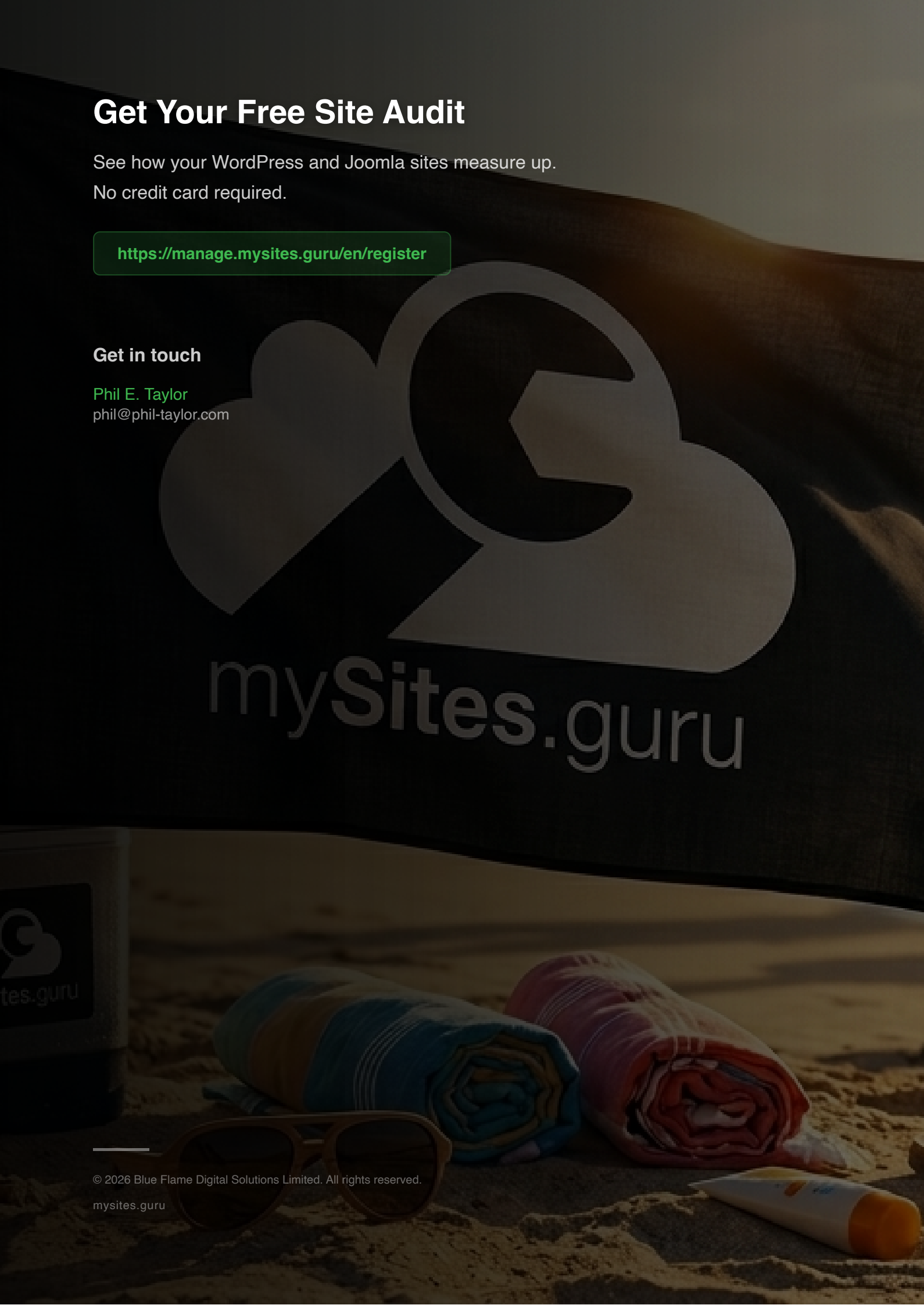
Shared code that ships to multiple CMS platforms needs security advisories for every affected platform, not just the one with the best CVE pipeline. When a vulnerability is discovered in Joomla/WordPress cross-platform code, the vendor and the researcher should coordinate disclosure so Joomla site operators get the same warning WordPress site operators do.

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