mySites.guru

J2Store 3.3.22, 4.0.22 and 4.1.7 fix five flaws we reported

J2Store 3.3.22, 4.0.22 and 4.1.7 fix five flaws mySites.guru reported, including anonymous PayPal order confirmation and a 9.4 backend escalation.

Phil E. Taylor | 1 September 2026

J2Commerce published a security release for the J2Store Joomla extension on 31 August 2026, fixing five vulnerabilities in `com_j2store`. We found and reported all five, and the vendor credits mySites.guru in its advisory. The fixed builds are **3.3.22** on the Joomla 3 branch, **4.0.22** on 4.0.x and **4.1.7** on 4.1.x, all published the same day.

The timing is the awkward part. J2Commerce shipped its previous security release ten days earlier, on 21 August, closing six unrelated flaws found by other researchers. Anyone who patched then did exactly the right thing and is still exposed, because 3.3.21, 4.0.21 and 4.1.6 are all affected by this second set.

> **Update to the fix for your own branch, not the highest number**
>
> J2Store patches three branches in parallel, so the correct target depends on which one you are on: **3.3.22** for Joomla 3, **4.0.22** for 4.0.x, **4.1.7** for 4.1.x. Moving from 4.0.21 to 4.1.7 is a branch change, not an update, and 4.1.7 is not an upgrade path for a Joomla 3 site at all.

TL;DR

TL;DR: Five vulnerabilities in the J2Store Joomla extension, all reported by mySites.guru, are fixed in 3.3.22, 4.0.22 and 4.1.7. Three need no login: an anonymous PayPal callback could confirm an unpaid order or fail a real one (8.7), an anonymous request could insert or overwrite any customer's cart record (8.8), and a crafted link fired script through the product-tags filter (5.3). One needed only an ordinary customer account and returned a guest checkout customer's name, address and phone (7.1). The worst, scored 9.4, needed only a Joomla backend login of any kind, with no J2Store permission whatsoever, and reached table truncation and traversal-based SQL file execution. Every build below the fix for its branch is affected, including the 21 August security release. The five CVE ids are reserved with the Joomla CNA but not yet published, so these scores are the vendor's. If you manage Joomla shops, mySites.guru already flags every connected J2Store install below the fix version for its own branch.

What the Five J2Store Flaws Actually Were

All five sit in `com_j2store` and all five affect every supported branch, because the vulnerable code is shared between them. Ordered by the vendor's own scoring:

CVE	Score	What it allowed	Login needed
CVE-2026-78069	9.4 Critical	Table truncation and traversal-based SQL file execution through the admin Apps controller	Any Joomla backend account
CVE-2026-78064	8.8 High	Insert or overwrite any user's or session's cart record	None
CVE-2026-77999	8.7 High	Confirm an unpaid order, or fail a legitimate one, through the PayPal callback	None
CVE-2026-78065	7.1 High	Read a guest customer's name, street address and phone from the address editor	Any customer account
CVE-2026-78000	5.3 Medium	Reflected XSS through the product-tags filter fields	None

Two of these are worth more than a table row, because the mechanism behind each one is a mistake that is easy to repeat in any Joomla extension.

Any Joomla Backend Login Could Truncate the Store's Tables

The 9.4 is an authorization check that was never written, sitting behind a framework default that opens rather than closes.

J2Store's administrator Apps controller accepts an `appTask` parameter and delegates the work to an app-plugin controller. Nothing along that delegation path checks whether the caller holds any `com_j2store` permission. That would still be survivable if the framework refused unmatched tasks, but the component's `fof.xml` has no

`<view>` ACL entries under its `<backend>` node at all, and with nothing declared the framework's default for an unmatched task is allow.

The practical result is a privilege escalation with an unusually low starting point. The only thing standing between an anonymous visitor and this code is Joomla core's administrator login wall, which is doing its own job and knows nothing about `com_j2store` permissions. Once any account is through that wall, for any reason, it could reach `#__j2store_*` table truncation and traversal-based execution of SQL files. An account you created so a client could manage their events calendar was enough to wipe their shop.

> **An empty ACL node is not a locked door**
>
> The pattern to take away from this one is general. If your component's ACL configuration declares nothing for a view, check what your framework does with a task it cannot match, because "no rule" and "deny" are not the same thing and the difference is invisible in a code review that only reads the controller.

The PayPal Callback That Verified Nothing

The 8.7 is the one a shop owner feels in the accounts rather than in the logs.

J2Store's PayPal IPN listener is supposed to call PayPal back, ask whether a payment notification is genuine, and act on the answer. Before the fix it did three things that each defeated that on their own. It treated an `UNVERIFIED` response, and in fact anything that was not literally `INVALID`, as valid. It made the verification request with `CURLOPT_SSL_VERIFYPEER` disabled. And it stored the verdict in a field that nothing downstream ever read, so order processing continued regardless of what came back.

The amount check had a separate hole. The comparison between what was paid and what was owed only ran when `mc_gross` arrived as a positive number, and `floatval(null)` is `0`, so simply leaving that field out of the callback body skipped the check completely.

Put together, an unauthenticated request to the callback endpoint could confirm an order that nobody paid for, or push a genuine customer's paid order into a failed state. If you ran an affected build with PayPal enabled, that is the thing worth auditing before you move on: orders that changed to CONFIRMED or FAILED with no matching PayPal transaction behind them.

Which J2Store Versions Are Affected?

Every build below the fix version for its own branch, on all three branches. There is no lower bound worth quoting, because the vulnerable code predates every version anyone is realistically running.

Branch	Affected	Update to
Joomla 3 (J2Store 3.3.x and earlier)	3.3.21 and below	**3.3.22**
J2Store 4.0.x	4.0.21 and below	**4.0.22**
J2Store 4.1.x	4.1.6 and below	**4.1.7**

J2Commerce 6 is a separately rewritten codebase for Joomla 6 and is not covered by this advisory.

The three fixed builds are worth staring at for a second, because they are the reason a lot of tooling will get this wrong.

Why One Version Range Cannot Cover J2Store's Three Branches

`4.0.22` and `3.3.22` both sort below `4.1.7`. So the obvious rule, "anything below 4.1.7 is vulnerable", tells a Joomla 3 shop that correctly installed 3.3.22 that it is still at risk, and keeps telling it that through every future scan, because no build on that branch will ever climb above 4.1.7. The site owner then either ignores the warning or goes looking for an update that does not exist for their branch.

This is not hypothetical for us. It is why the J2Store entries in our Joomla vulnerability rules are three rules rather than one, split on branch boundaries that cannot overlap:

```
below 3.3.22                -> Joomla 3 branch
4.0.0 and above, below 4.0.22 -> 4.0.x branch
4.1.0 and above, below 4.1.7  -> 4.1.x branch
```

We learned that the expensive way on a different extension. Convert Forms fixed one flaw in 4.4.16 for Joomla 3 and 5.2.3 for Joomla 4 and up, and a single range written across both told thirty correctly patched sites they were vulnerable until a customer told us otherwise. Any vendor maintaining a Joomla 3 branch alongside a modern one produces the same trap, and J2Store maintains two of them.

How Do I Find Every Affected J2Store Install?

By hand it means logging into each Joomla site, opening the extensions list, reading the J2Store version, working out which branch it belongs to and comparing it against the right one of three targets. For one shop that is five minutes. For an agency with thirty Joomla sites it is the kind of job that gets postponed, which is precisely what the numbers below show happening.

With mySites.guru, every connected Joomla site reports its full extension inventory, so J2Store installs across the whole account list on one screen with their versions. The three branch rules for this advisory are live now, alongside the three for the 21 August release, so an affected shop is flagged with the fix version for the branch it is actually on rather than the highest number in the advisory. If you want to see that against your own sites before paying for anything, the free audit covers it.

What the Connected J2Store Stores Actually Look Like

This is the part we can measure and most write-ups cannot. Across the Joomla sites connected to mySites.guru that run the J2Store component and reported a readable

version in the last thirty days:

93%
below the fix for their own branch
on the day the advisory published

68%
of those are on the Joomla 3 branch
3.3.x and older

74%
of those never applied the 21 Aug fix
two advisories behind

7%
already patched
on 3.3.22, 4.0.22 or 4.1.7

Measured 1 September 2026 across connected Joomla sites running com_j2store with a snapshot in the previous 30 days. Percentages of that group, not of all managed sites.

The 74% is the figure that should bother anyone running a Joomla shop. Three quarters of the affected stores are not one security release behind, they are two: still below the 21 August build that fixed an unauthenticated file upload the vendor confirmed had already been exploited in the wild. Those shops did not miss this advisory. They missed the last one too, and this one arrived before anybody noticed.

That pattern is why an extension inventory beats a mailing list. A shop owner reading a vendor advisory has to already know they run the extension, already know which branch, and already be reading. An inventory does not require anyone to be paying attention on the day.

Was Any of This Being Exploited?

We have no evidence of exploitation of these five before the fix shipped, and no proof of concept has been published for any of them. This post deliberately describes mechanisms rather than requests.

The honest caveat is that four of the five leave very little behind. A guest address read through the address editor looks like an ordinary page view. A cart row inserted anonymously looks like a cart row. The one that does leave a trace is the PayPal

callback, because the order state changes, so that is the one to go back through if you ran an affected build with PayPal enabled.

The 21 August release is a different matter, and worth restating for the three quarters of shops still below it: the vendor confirmed that the file upload flaw in that set had been exploited in the wild before the patch shipped. If a shop is on 3.3.20 or below, 4.0.20 or below, or 4.1.5 or below, treat it as needing a look rather than just an update. Our guide to checking a Joomla site's database and file integrity covers what to review.

Credit Where It Is Due

Two things J2Commerce did here are worth saying plainly, because plenty of vendors do neither.

They patched the Joomla 3 branch on the same day as the modern ones. J2Store's users skew heavily toward Joomla 3, as the 68% above shows, and a vendor who fixes only the current branch effectively strands most of their install base. J2Commerce has now done the simultaneous three-branch release twice in ten days.

They also named the reporter. The advisory credits Phil Taylor of mySites.guru with discovery and responsible disclosure of all five issues, and thanks the Joomla Security Strike Team. We have written before about what a good Joomla extension disclosure looks like, and about vendors who shipped our fixes without ever saying where they came from. This one is on the right side of that line.

The five CVE ids are reserved with the Joomla CNA. When the records publish, the scores and affected ranges quoted here may shift, and we will update this post if they do.

9.4
CVSS 4.0

CRITICAL

J2Commerce's own advisory, 31 August 2026 · CVE-2026-78069

The worst of the five. Any account that can reach the Joomla administrator login, holding no J2Store permission at all, could trigger table truncation and traversal-based SQL file execution against the shop. The CVE record is reserved with the Joomla CNA and not yet published, so this score is the vendor's rather than a CNA assessment, and the vector's PR:L reflects that a backend login is needed even though no J2Store rights are.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H`

Backend login, any privilege | No J2Store permission needed | Data destruction | Reaches file execution

Timeline

2026-08-21 — **J2Commerce ships 3.3.21, 4.0.21 and 4.1.6 for a different six flaws**

Six CVEs found by other researchers, including an unauthenticated file upload the vendor confirmed had been exploited in the wild. This is the release most affected shops are still sitting one step below.

2026-08-25 — **Five issues reported privately to J2Commerce**

The PayPal callback forgery, the reflected XSS, the anonymous cart tampering and the guest-address IDOR, all four proven live against a test installation. The fifth, the Apps delegation chain, was reported as shielded only by accident, with a warning that any change to fof.xml would expose it.

2026-08-25 — **J2Commerce acknowledges the report the same day**

Olivier Buisard confirms receipt four and a half hours later and says the issues will be resolved.

2026-08-31 — **J2Commerce ships 3.3.22, 4.0.22 and 4.1.7 for all five**

All three branches patched the same day. The advisory credits Phil Taylor of mySites.guru with discovery and responsible disclosure of all five issues, and thanks the Joomla Security Strike Team. The vendor also re-assessed the Apps delegation chain as reachable by any authenticated backend user and scored it 9.4, higher than the report treated it.

2026-09-01

mySites.guru flags every affected connected store

Three new vulnerability rules, one per release branch, so an affected site is told the fix version for the branch it is actually on. The five CVE ids are reserved with the Joomla CNA but not yet published at MITRE.

Further Reading

- A month of Joomla security disclosures - the wider set of extension flaws we reported over one month, of which this is a continuation.
- Exposed invoices and order forgery in EasyStore - the same shape of bug in another Joomla shop extension: guessable ids, orders marked paid for free.
- Cotton Cloud patched the login, then the data - what an ownership check that only half runs looks like, which is exactly the guest-address gap described here.
- Why AJAX endpoints are a CMS security blind spot - the recurring pattern behind the cart tampering: a task reachable by anyone, with the framework's CSRF check quietly not applying.
- CWE-862: Missing Authorization and CWE-639: Authorization Bypass Through User-Controlled Key - the canonical definitions for the two worst issues here.
- J2Commerce security announcement - the vendor's own advisory, with the full CVSS vectors.

Frequently Asked Questions

Which J2Store versions fix these five vulnerabilities?

J2Store 3.3.22 on the Joomla 3 branch, 4.0.22 on the 4.0.x branch and 4.1.7 on the 4.1.x branch, all published on 31 August 2026. Every build below the fix version for your branch is affected, and that includes 3.3.21, 4.0.21 and 4.1.6, which were themselves security releases ten days earlier. Install the build that matches the branch you are on. Do not move sideways onto a higher-numbered branch to escape the flaw, because 4.1.7 is not an upgrade path for a Joomla 3 site.

What is the worst of the five J2Store flaws?

CVE-2026-78069, scored 9.4 Critical in the vendor advisory. The administrator Apps controller in the J2Store Joomla extension delegates work to app-plugin controllers without ever checking com_j2store permissions, and the component's fof.xml declares no backend view ACL, so the framework defaults an unmatched task to allow rather than deny. Any account that can log into the Joomla administrator, holding no J2Store permission at all, could trigger table truncation and traversal-based SQL file execution. A backend login for an unrelated component became a route to destroying the shop's data.

Do any of these J2Store flaws work without logging in?

Three of the five do. The PayPal callback forgery, the cart-record tampering and the reflected XSS all need no account. The guest address disclosure needs any ordinary logged-in account, which on a shop with open customer registration is trivial to obtain. The 9.4 Critical needs a Joomla backend login, but not one with any J2Store permission, so an account created to manage an unrelated component is enough.

Could someone have got free orders out of a J2Store shop?

Before the fix, yes. The PayPal IPN listener treated an UNVERIFIED response as valid, ran its verification request with SSL peer verification disabled, and stored the verdict in a field nothing downstream read, so processing continued whatever the answer was. Separately, leaving the mc_gross field out of the callback skipped the paid-amount comparison entirely. An anonymous request could mark an order confirmed without any money moving, or fail a legitimate one. If you ran an affected build with PayPal enabled, review recent orders for CONFIRMED or FAILED transitions with no matching PayPal transaction.

Are these five CVEs published yet?

Not at the time of writing. All five ids are reserved with the Joomla CNA but the records are not yet live at MITRE, so the CVSS scores quoted here come from the vendor's own advisory rather than from a published record. Scores sometimes move when the CNA publishes, and affected ranges occasionally widen, so treat these as the vendor's assessment for now.

How do I find every J2Store install across the sites I manage?

Manually you would log into each Joomla site and read the installed extensions list, which is slow and gets skipped. mySites.guru keeps an extension inventory for every connected site, so searching for J2Store returns every install with its version on one screen, and any site below the fix version for its own branch is already flagged with that branch's correct target. The rules for both August advisories are live now.

Does updating J2Store undo anything that already happened?

No. Updating closes the routes; it does not reverse what was done through them. On a shop that ran an affected build, check orders for confirmations with no matching payment, review who holds a Joomla administrator login of any privilege level, and treat guest checkout addresses as potentially read. The address disclosure and the cart tampering both leave little trace in a normal access log.

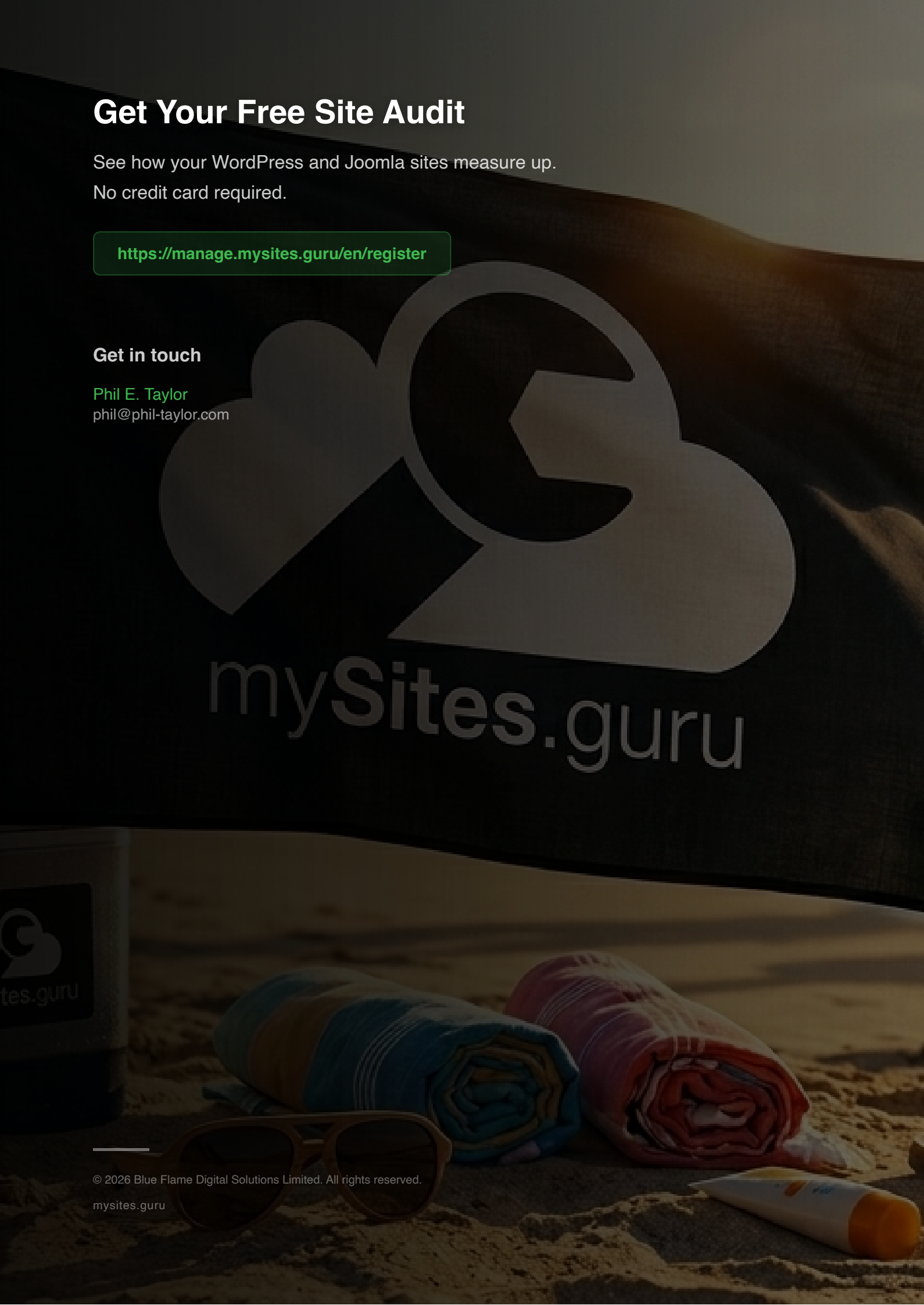
Written and edited by a human, with AI assistance. Our approach to AI

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.