mySites.guru

DPCalendar 10.12.0 fixes an SQL injection and an XSS

Digital Peak fixed a blind SQL injection and a stored XSS in DPCalendar 10.12.0, backported to 8.19.5 for Joomla 3. Both need a logged-in user.

Phil E. Taylor | 3 October 2026

Digital Peak released DPCalendar 10.12.0 today, with a security section that named two issues and gave no detail beyond a severity rating. So we did what we usually do and diffed the packages.

This is the second security release for this Joomla extension in six weeks. The first was ours: we reported an unauthenticated SQL injection in July, and Digital Peak fixed it in a day. This one is not ours. Both issues were reported by an independent researcher, Toan Le, and both need somebody logged in, which makes this a different kind of problem from July's.

TL;DR

- **DPCalendar 10.12.0** fixes a blind SQL injection (vendor-rated High) and a stored cross-site scripting flaw (vendor-rated Medium). Both fixes are backported to **8.19.5** for the Joomla 3 branch
- The SQL injection is reached by **saving a Joomla article** that contains a DPCalendar tag, so it needs article-edit permission. The XSS needs permission to create a DPCalendar location
- Neither is reachable by an anonymous visitor. No one can walk in off the internet and trigger either one
- **No CVE has been assigned yet** for either issue
- The root cause of the SQL injection is worth understanding: the sort column was passed through the database escaping function, which protects values inside quotes and does nothing at all for a column name
- Across the DPCalendar sites we can currently see, **more than four in five** are still on a version below this fix. More concerning, about **one in six** is still missing July's fix, which closed a flaw an anonymous visitor could use

What Digital Peak fixed in DPCalendar 10.12.0

The vendor's release announcement lists both issues by internal tracker number:

- **#12206**, a blind SQL injection triggered by saving an article, needing update permission for articles, rated **High**
- **#12203**, a location title rendered into a data attribute without escaping, leading to cross-site scripting, needing create permission in DPCalendar, rated **Medium**

Digital Peak also states that the site itself cannot be compromised through these, that files are safe, and that they have no information suggesting data was stolen, because the finder contacted them directly. We found nothing to contradict that: there is no public proof-of-concept, no exploit code, and no report of exploitation in the wild for either issue.

How the SQL injection works, and why escaping did not stop it

This one is a good teaching case, because the vulnerable code looks defended.

DPCalendar's front-end events model builds a query and then adds a sort clause. Before 10.12.0, it took the sort column and direction out of the model's state and passed each through the database escaping function on the way into the query.

That reads like protection. It is not, and the reason is worth spelling out, because the same misunderstanding shows up across a lot of PHP.

An escaping function exists to make a **value** safe once it sits inside quotes. It handles the characters that would let a value break out of its quoting. A sort column never sits inside quotes: it is an identifier, part of the grammar of the statement rather than data inside it. So the escaping ran, found nothing it was designed to change, and passed the text through into the query as instructions.

The fix in 10.12.0 checks the sort column against the model's existing list of columns that actually exist, and the direction against a short list of permitted values, falling back

to a safe default when either fails. That is the correct shape for this problem: an allowlist, not a filter.

Where the attacker-controlled value comes from

The part that turns this from a code smell into a vulnerability is how the sort value reaches the model.

The sort parameter that arrives in a normal web request was already validated against that same list of real columns, in both the vulnerable and the fixed version. We checked, because it changes the advice considerably. That path was never the problem.

The route that was open ran through the DPCalendar content plugin. That plugin reads DPCalendar tags inside Joomla article text and turns the options written in the tag into settings on the events model, including the sort column and direction, with no validation on the way through. So the attacker is not a passing visitor tampering with a URL. The attacker is somebody who can save an article.

That also explains the practical workaround. Because the request path was already safe and the plugin path was not, disabling the DPCalendar content plugin closes this specific route while leaving calendar menu items and modules working.

We are describing the mechanism at the level the vendor did and not publishing the tag syntax or a working payload, because most sites running this extension have not updated yet.

The cross-site scripting flaw in DPCalendar location titles

The second issue is simpler. DPCalendar renders a location’s title into an HTML attribute that its map JavaScript reads. In the versions before 10.12.0, several templates wrote that title into the attribute raw.

If a title contains the characters that end an attribute, it stops being text and becomes markup, which is the whole of cross-site scripting. It is stored rather than reflected, so the payload sits in the database and fires for whoever views the page afterwards.

The fix has two parts, which is the right way to do it. On the way in, the location title field now runs through Joomla's configured text filter, so tags are stripped on save. On the way out, the templates escape the title before writing it into the attribute. Input filtering and output escaping solve different parts of the problem, and this release added both.

Creating a DPCalendar location is a permission, not something anonymous visitors can do, so this needs an account with location-create rights.

Which DPCalendar versions are affected?

Line	Affected	Fixed in
Current (Joomla 4.4.4 to 6.x)	Everything below 10.12.0	**10.12.0**
Joomla 3 branch	Everything below 8.19.5	**8.19.5** (security fixes only)
9.x	All of it	No patch. Upgrade to 10.12.0

The vulnerable code sits in the component's own front-end model and its location templates rather than in any edition-specific add-on, so this is not a Free-edition problem. If you run DPCalendar, you are on the list until you update.

The 9.x line is the awkward one, exactly as it was in July. There is no 9.x patch, and the route across is staged: 9.x to 10.0.0, then 10.6.0, then 10.12.0.

Who can actually exploit this?

This is the question that decides whether today is a busy afternoon or a routine update, and it depends entirely on your site.

On a brochure site where you are the only person who ever logs in, both of these are housekeeping. Patch on your normal schedule.

On a site with freelance writers, client staff who publish their own news, a membership tier that grants Author, or an old contractor account no one got round to deleting, the picture changes. The SQL injection is the difference between an account that can write a news post and an account that can read every user record and password hash in the database. Blind injection sounds like a limitation, and it is not much of one: a boolean oracle reads a database one character per request, and no one does that by hand.

So the useful exercise today is opening the user list on the sites that matter and asking who still has an account, and why, alongside patching.

What we see across the Joomla sites we manage

We record the installed version of every extension on every connected site, which lets us say something about how a release like this actually spreads, rather than guessing.

Looking only at sites that have reported in during the last 30 days, on the day of release:

- **More than four in five** DPCalendar installs are on a version below 10.12.0 or 8.19.5. That is normal for release day, and it is why we email affected customers directly rather than waiting for people to notice a version badge change in the mySites.guru dashboard
- About **one in six** had already taken the update within hours. Digital Peak's update channel moves faster than most, which is a credit to them
- Roughly **one in five** installs sit on the 8.x branch or older, meaning they run on Joomla 3. Joomla 3 reached end of life in August 2023, and even the paid extended support programme ended in February 2025. Digital Peak still ships security fixes for that branch, which is more than most vendors do, but the CMS underneath it has had no official security support for well over a year

- There are **81 distinct DPCalendar versions** in the wild across the sites we can see, and the oldest still running is a 4.x. That version predates every fix discussed here by years

We are not publishing site counts, because the size of the estate is not ours to hand out. The proportions are the useful part anyway.

The tail from July is the bigger problem

Here is the number that made us stop, and it has nothing to do with today's release.

Six weeks after Digital Peak shipped July's fix, and after we emailed every affected customer directly, **about one in six** of the DPCalendar installs we can see is still on a version below 10.11.2 or 8.19.4.

Those sites have a worse problem than the one this release fixes. July's flaw was CVE-2026-57831, CVSS 4.0 8.7, and it needed no login at all. An anonymous request against a public events feed read the database. Today's SQL injection at least requires an account with article rights.

If you are reading this and you have not touched DPCalendar since June, the version to worry about is not 10.12.0. Get to 10.11.2 or 8.19.4 first, because that is the one an attacker can reach without knocking.

Credit where it is due: a second fast fix

We were complimentary about Digital Peak in July, and nothing here changes that.

They shipped that fix inside 24 hours, over a holiday break, outside their normal release schedule. This time they fixed both issues in the scheduled monthly release, backported them to a branch supporting a CMS that has been end-of-life for three years, published a security section naming both issues and their severities, and credited the researcher by name with a link to his profile.

The one thing we would ask for is more detail in the announcement itself. “Security: High” with no description is what sent us to a package diff. Site owners deciding whether to interrupt their afternoon deserve to know that both issues need an authenticated user, and that fact was in the announcement only if you read to the security section rather than the changelog line.

For the record, Digital Peak has no published security policy page that we could find, and no `security.txt`. For a vendor that handles reports this well in practice, that is a gap worth closing.

One claim from July does not hold up

When Digital Peak fixed our July flaw, their advisory described it as the first security vulnerability reported in DPCalendar since the component first shipped in 2012. We repeated that at the time, because it was their statement to make. It is not accurate, and we would rather correct our own record than let it stand.

DPCalendar had a cross-site scripting vulnerability disclosed in February 2024, tracked as CVE-2024-21727 and assigned by the Joomla CNA, affecting versions 8.0.0 to 8.14.0. That is public record, and it predates July’s SQL injection by more than two years.

This is not a mark against the fixes, which have been fast and complete. It matters because “first since 2012” gets repeated, and an extension’s real security history is exactly what tells you whether to keep it patched and watched. DPCalendar now has at least four separate issues on the public record: the 2024 XSS, our July SQL injection, and the two Toan Le reported this week. That is a normal number for a large, actively used extension, and the useful takeaway is the opposite of reassuring folklore about a clean sheet: treat every extension as something that will need updating, because sooner or later it will.

Toan Le is auditing Joomla extensions at pace

The finder here is worth noting, because it fits a pattern we wrote about earlier this month.

Toan Le's public work since June 2026 includes CVEs in JoomGallery (an IDOR with stored XSS, and a password-protected category bypass), J2Commerce (stored XSS through a cookie filter bypass), PhocaCart (an unauthenticated SQL injection scored 9.3, plus two stored and reflected XSS issues) and PhocaCommander (three path traversal flaws). That is a systematic sweep of widely installed Joomla extensions by one researcher, in the same window we have been running our own.

This is good news, and it has a practical consequence. The rate at which Joomla extension vulnerabilities are being found and disclosed has gone up sharply this year. The extensions have not suddenly got worse; more people are looking. If your update process assumes a couple of extension security releases a year, it is calibrated for a quieter era than the one we are in.

How do you update DPCalendar safely?

DPCalendar updates through Joomla's own extension updater, so the mechanics are ordinary. The parts worth care:

1. **Take a backup first**, particularly on the 9.x line where you are doing a staged upgrade rather than a point release
2. **Check your Joomla version supports the target.** The 10.x line needs Joomla 4.4.4 or newer. If you are on Joomla 3, your target is 8.19.5, not 10.12.0
3. **Update on a staging copy first** if the site runs a heavily customised calendar. 10.12.0 is a feature release as well as a security one, adding article creation from events and tag display in list views
4. **Check your template overrides.** If you have overridden any of the DPCalendar location templates, your overrides still contain the unescaped output, and updating the extension will not fix a copy sitting in your template. This is the single most likely way to update and stay vulnerable

5. **Enable automatic updates** so the next one arrives without you doing anything. We wrote up how to turn on auto-updates for any Joomla extension

That fourth point is the one that catches people. Overrides are copies, and a security fix in a template never reaches a copy.

How do I find every DPCalendar site I manage?

If you run one site, open its extension manager and look.

If you look after thirty, that approach is how things get missed. Searching for the extension by name in the mySites.guru Extension Inventory lists every connected site running DPCalendar and the version each one reports, so you can sort by version and work down the list. Version tracking across every connected site is part of the mySites.guru subscription, along with alerts when an installed extension version matches a known vulnerability rule.

That is also how we built the numbers in this post, and how we knew who to email about it this afternoon.

What to do right now

- **Update to 10.12.0**, or **8.19.5** if the site runs Joomla 3
- **Check you are past July's fix first.** If a site is below 10.11.2 or 8.19.4, it has an unauthenticated SQL injection open, which matters more than either issue in this release
- **If you cannot update today**, disable the DPCalendar content plugin to close the SQL injection route, and treat that as a few days of breathing room rather than a fix
- **Check your template overrides** for copies of the DPCalendar location templates
- **Look at who holds accounts** on any site where people other than you can edit articles or create locations, since that is what both flaws require

- **If a site was on a vulnerable version for a long time** and handles data you would not want read, review your Joomla database security and check for rogue admin accounts

---

Timeline

2026-07-12

mySites.guru reports an unauthenticated SQL injection in DPCalendar

A different flaw from the two in this post: the public events feed took an author filter and placed it into the query without casting it to an integer, so an anonymous visitor could read any table. We disclosed it privately with all public detail withheld.

2026-07-13

Digital Peak ships 10.11.2 and 8.19.4 within 24 hours

Built, tested and released over a holiday break, outside their normal fourth-Thursday schedule. The fix cast the author filter to an integer on every path.

2026-07-15

The Joomla CNA assigns CVE-2026-57831

CVSS 4.0 8.7 High, affected range 8.18.0 to 10.11.1, crediting Phil Taylor of mySites.guru as the finder.

2026-08-27

Digital Peak ships 10.12.0 and 8.19.5, fixing two issues found by Toan Le

A blind SQL injection in the events query's sort clause, reachable from a saved article, and a stored cross-site scripting flaw in location titles. Both need an authenticated user. The vendor reports no evidence of exploitation.

2026-08-27

No CVE assigned yet for either issue

Digital Peak's announcement identifies them only by internal tracker numbers. Assignment through the Joomla CNA commonly follows a release by several days.

Further Reading

- The unauthenticated SQL injection we found in DPCalendar in July - a different flaw in the same events query, and the one to check first if you are running an older version.
- We are not the only ones auditing Joomla extensions - the wider pattern this release fits into.
- Why AJAX endpoints are a CMS security blind spot - the recurring public-endpoint pattern behind flaws like these.
- How to check your Joomla database security - what to review if a vulnerable version was live on a site handling real data.
- Find rogue admin accounts in Joomla - the check worth running whenever a flaw depends on who holds an account.
- CWE-89: SQL Injection and CWE-79: Cross-site Scripting - the official references for both weakness classes.

Frequently Asked Questions

What did DPCalendar 10.12.0 fix?

Two security issues reported to Digital Peak by researcher Toan Le. The first is a blind SQL injection, rated High by the vendor, reached by saving a Joomla article that contains a DPCalendar tag. The second is a stored cross-site scripting flaw, rated Medium, where a DPCalendar location title was written into an HTML attribute without being escaped. Both fixes were backported to DPCalendar 8.19.5 for the Joomla 3 branch.

Do these flaws need a logged-in user?

Yes, and that is the main thing separating this release from the DPCalendar flaw we reported in July. The SQL injection needs permission to edit an article. The cross-site scripting flaw needs permission to create a DPCalendar location. Neither can be triggered by an anonymous visitor, so how much this matters depends entirely on who holds accounts on your site.

Which DPCalendar versions are affected?

Every version below 10.12.0 on the current line, and every version below 8.19.5 on the Joomla 3 branch. The 9.x line has no patch at all, so those sites need the staged upgrade to 10.12.0. The vulnerable code is in the component's own front-end model and location templates rather than in any edition-specific add-on, so this is not limited to the Free edition.

Is there a CVE for these two issues?

Not at the time of writing. Digital Peak's release announcement names both issues by their internal tracker numbers and gives no CVE. That may still change, since CVE assignment through the Joomla CNA often follows a release by days. Treat the absence of a CVE as a paperwork gap rather than a verdict on severity.

How do I find every DPCalendar site I manage?

Searching the extension by name in the mySites.guru Extension Inventory lists every connected site running it, with the version each one reports, so you can work through them in one pass instead of logging into each site to check. Version reporting across every connected site is part of the mySites.guru subscription.

What can I do if I cannot update immediately?

Disable the DPCalendar content plugin in Joomla's Plugins manager. The SQL injection is reached through the DPCalendar tag that this plugin reads inside article text, and the request-based sort parameter was already validated, so turning that one plugin off closes the route. You lose any calendar embedded inside article text; calendar menu items and modules keep working. This buys time and does not replace the update.

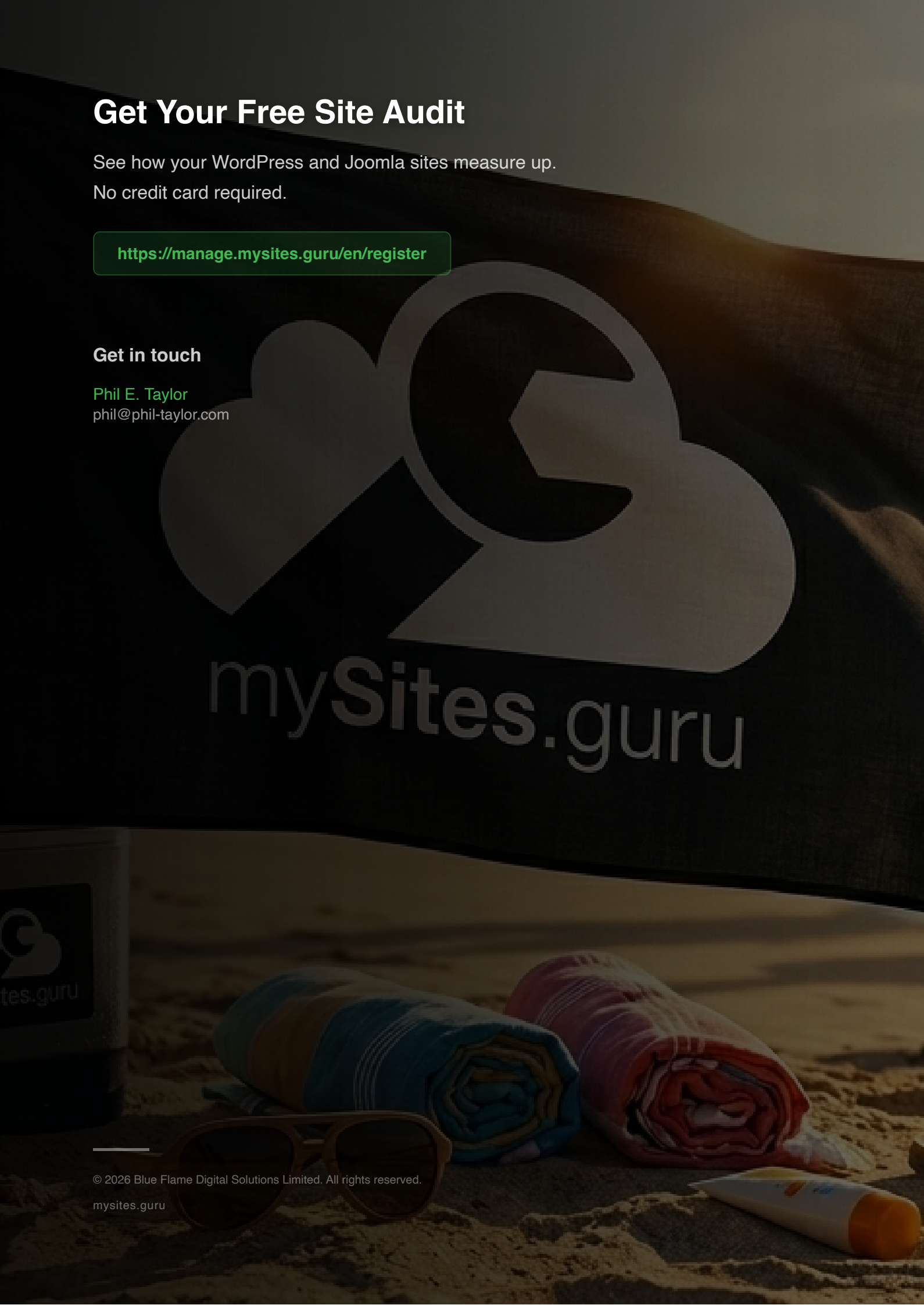
Written and edited by a human, with AI assistance. Our approach to AI

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.