mySites.guru

Event Gallery 6.5.0 Hides Eight Security Fixes in 46 Bug Fixes

Event Gallery 6.5.0 fixes a path traversal, an upload CSRF and a reflected XSS in Joomla. The vendor has since rewritten its notes to lead with security.

Phil E. Taylor | 26 September 2026

Sven Bluege released Event Gallery 6.5.0 for Joomla on 26 September 2026, and it is a security release. Before 6.5.0, a page on another website could make a logged-in editor upload images into a gallery event and replace existing ones, a crafted link could run script in an editor's session, and the identifiers of carts and orders in the image shop could be worked out from the time they were created.

The release page does not put it that way. The notes sit behind a collapsed More information button, run to 8,673 words, and file the security fixes among 46 bug fixes in the same even tone as a PayPal option and a German mail template. Nothing on the page tells a site owner to update today.

What to do now

Update Event Gallery to 6.5.0 on every Joomla site that runs it, Core and Extended alike. 6.5.0 needs Joomla 5.4 or later, so a site still on Joomla 3 or 4 has to upgrade Joomla first. If the site overrides the upload layout in its template, update the override too, or every upload will be rejected with an invalid token message.

Update, 26 September 2026: the release notes now lead with security

Following the first publication of this blog post, in response, Sven Bluege rewrote the 6.5.0 release notes the same afternoon. They now open with "This is a security release. Update every site to 6.5.0.", say that every earlier version is affected and that 6.5.0 needs Joomla 5.4 or Joomla 6, and send sites on older Joomla to a Security Advisories chapter in the manual. A new Security Fixes section lists five vulnerabilities, each with its own advisory ID and severity:

- EGSA-2026-01, path traversal in Clear Cache (severity 6.5). A backend user allowed to manage Event Gallery, which in Joomla's default permissions is every Administrator and not only Super Users, could make Clear Cache delete any folder

the web server can write to, up to the whole site. Our original post did not cover this one

- EGSA-2026-02, cross-site scripting and open redirect on the frontend upload page (6.1), affecting 3.11.4 to 6.0.0
- EGSA-2026-03, forged uploads (5.4)
- EGSA-2026-04, forged cart changes (4.3). Adding an image to the cart and removing it needed no token, so a page on another site could change a visitor's cart
- EGSA-2026-05, forged clean-up in the backend (4.3)

The guessable order identifiers, the test mail button, the backend picker requests and the unescaped folder name are now listed separately as hardening without a known vulnerability, which is why the vendor counts five where we counted eight. This is the change we asked for in the last section of this post, made within hours. The sections below describe the notes as they stood when 6.5.0 came out. The advice has not changed: update every site to 6.5.0.

The Joomla CNA will soon be issuing CVE numbers for these issues, and we will add them here when they are published.

TL;DR

- **Event Gallery 6.5.0** fixes eight security issues. The upload CSRF is present in both earlier releases we checked, 5.7.8 and 6.0.0
- **Image upload CSRF:** neither the backend nor the frontend upload checked Joomla's form token, so a malicious page could upload or replace images in an event through a logged-in editor. Uploads are still limited to images and mp4 video, so there is no route to running code
- **Reflected XSS:** the Back link on the frontend upload page printed a URL parameter as it came, so a crafted link could redirect an editor or run script in their session

- **Guessable order IDs:** cart and order identifiers were derived from the creation time. Orders created before the update keep their old identifiers
- Several backend actions, from clean-up links to test mails, were missing token or permission checks
- No CVE and no Security heading. The fixes are in the Bug Fixes list, and the only highlight that mentions them is one word: “Safer.”
- About a third of the affected sites we monitor are on Joomla 3, where 6.5.0 will not install
- mySites.guru flags every connected Joomla site running Event Gallery below 6.5.0

The Event Gallery 6.5.0 release notes run to 8,673 words

Open the 6.5.0 release page and you see a version number, a release date, two download links and a small button labelled More information. Press it and the notes unfold: eight highlights, ten migration hints, 21 new features, 15 minor changes and 46 bug fixes, 8,673 words in all. It is well written, too. Every entry says what used to happen, what happens now and what, if anything, you need to change.

What it never does is sort the entries by how much they matter. There is no Security heading. The word “vulnerability” does not appear. The eight highlights lead with buying several images at once, a new cart, PayPal Checkout and new mails for buyers, and the security work comes last, as a single bullet that starts with the word “Safer.” In the Bug Fixes list the first security entry is number 8, and the upload CSRF, the fix with the widest reach, is number 39 of 46, between a fix for the upload page of Flickr and Google Photos events and the fix for the test mail button.

The entries are accurate. The one for the Back link says, in plain words, that a prepared link could “run a script in the session of the editor who clicked it”. But you only read that sentence if you expand a collapsed panel and scroll past more than 8,000 words to reach the upload fix, and at no point does the page connect any of it to an action.

“Safer. The upload, the test mail, the clean-up links and the background requests of the backend check the form token now, and new carts and orders get identifiers which can no longer be guessed.”	“Security release. Before 6.5.0 a malicious page could upload or replace images through a logged-in editor, and a crafted link could run script in their session. Update every site now.”
Read as hardening. Updated with the next batch.	**Updated today.**

The line on the left is the vendor's, word for word from the Event Gallery 6.5.0 highlights. The line on the right is ours, written from the vendor's own Bug Fixes entries and our reading of the code. They describe the same release.

Most people looking after more than a handful of Joomla sites triage extension updates by skimming the top of the notes. A release led by shop features reads as a feature release, and a feature release on a live photo shop is the kind of update that gets scheduled for a quiet week, not applied the same morning. We made the same point about Helix3 shipping a critical fix as “Security Update”, T4 Page Builder calling an open mail relay “Safer recipients” and AcyMailing filing two security fixes under Bug fixes. The Joomla project’s own guidance for extension developers handling a security report asks for the security content to be separated out and named. The fix here is small: move the eight entries under their own heading at the top, and add one sentence saying which versions are affected and that sites should update.

What the Event Gallery 6.5.0 security fixes close

Our reading, not our discovery

Sven Bluege found and fixed these issues himself; we did not report them. We confirmed the upload, Back link and identifier findings by comparing the 5.7.8, 6.0.0 and 6.5.0

packages. The severity is our own assessment, and there is no CNA score to compare it with. We are not publishing request shapes, because most installs have not updated yet.

The Joomla image upload had no CSRF token

In 6.0.0 and 5.7.8, the upload task in both the backend and the frontend controller passed the request straight to the model. The model checked that the user had Joomla's edit permission for Event Gallery and nothing else. It never checked the form token, the value Joomla puts in every form so the server can tell a request the user made from one another website made on their behalf.

That makes the upload a classic cross-site request forgery. An editor, or a frontend publisher who uploads from the site, visits a page that posts a file to their own site's upload task in the background, and their browser sends their session cookie with it. The file goes into the named event, and if an image of the same name is already there, it is replaced. On a photo shop that sells prints of an event, that lets an attacker swap the pictures customers are paying for.

There is a limit to the damage. Event Gallery checks the extension against an allow-list of jpg, gif, png, jpeg, webp and mp4, checks the file's actual content type as well, and cleans the file name. We found no route from this upload to running code on the server. 6.5.0 adds the token check to both controllers, and a site with a template override of the upload layout has to update that override, because the page now passes the token to the uploader script.

The Back link on the upload page was a reflected XSS

The frontend upload page offers a Back link, and before 6.5.0 its target came from a `return` parameter in the address, base64-decoded and printed into the page without escaping or checking. A crafted link could point Back at another website, or break out of the link and run script in the page, in the session of whoever opened it. The people who use that page are the site's editors and publishers, so the script runs with their rights.

6.5.0 only accepts a target on the site's own domain and leaves the link out otherwise. The same page also printed an event's folder name unescaped. Folder names saved through the backend are cleaned, so that one only matters if a name reached the database another way, and 6.5.0 escapes it too.

Cart and order identifiers could be worked out

Event Gallery built cart identifiers from PHP's `uniqid()`, which is derived from the current time, and turned the result into a 28-digit number. The vendor's notes spell out the consequence: anyone who knew roughly when an order was placed could work out its identifier. They also note that the number was too large for PHP to hold as an integer, so a single careless cast anywhere could collapse every identifier into one value and show one customer another's order.

The vendor says order download links were never exposed, because they use a separate random token. From 6.5.0 new carts and orders get a short prefix followed by 16 random bytes. Carts and orders that already exist keep their old identifier, so updating does not make historic orders harder to guess.

Backend actions skipped their token and permission checks

The remaining fixes are backend actions that trusted any logged-in administrator request. The two clean-up links on the overview page, which delete orphaned files and old carts, had no form token, so a prepared link on another website could trigger them. The test mail button on email templates had no token and no edit permission check. Sync Database, Thumbnail Creator and Clear Cache carried on after the token had expired or for users who could not manage the component, and three small backend requests that fill the content plugin's pickers and count missing thumbnails answered anyone logged into the backend. 6.5.0 checks the token and the permission on all of them.

Which Joomla sites can install Event Gallery 6.5.0?

Only sites on Joomla 5.4 or later, or Joomla 6. Event Gallery 6.5.0 is published for those versions alone, and there is no 5.x or 4.x maintenance release with the fixes, so a site on an older Joomla core has no Event Gallery version it can update to that closes these issues. That makes the release a bigger job than it looks for a large share of the sites that need it.

Across the Joomla sites connected to mySites.guru, 91% of Event Gallery installs were below 6.5.0 on the morning it came out, and 42% were on 6.0.0, the release before. Split the affected sites by Joomla core and the picture changes: 59% run Joomla 5.4 or later and can update in a couple of minutes, but about a third are on Joomla 3 and a further 7% on Joomla 4. The single most common version among those older sites is Event Gallery 4.3.2, from January 2023, the last release published for Joomla 3.10.

For those sites, the extension update is the easy half. The real work is getting off Joomla 3, which has been end of life since August 2023, and any gallery and shop extension that stopped receiving fixes at the same time is one more reason to schedule it.

How mySites.guru flags Event Gallery below 6.5.0

mySites.guru records the exact version of every extension on every connected Joomla site twice a day. Our Joomla vulnerability database had an entry for Event Gallery below 6.5.0 on the day the release came out, so each connected site running an older component is flagged on its dashboard and in its audit, whether it runs Core or Extended. The Event Gallery page of our vulnerability list shows the rule, and the vulnerable extension list explains how the flags work across every extension we track.

The same audit checks the Joomla core version, which is the part that decides how much work each flagged site needs. A site on Joomla 5.4 or later can be updated in bulk from one dashboard. A site on Joomla 3 or 4 goes on the upgrade list instead.

Joomla CMS Version Must Be Up-to-date

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

What should I do if I cannot update Event Gallery yet?

Reduce the number of people who can be used against the site until you can. Every issue except the order identifiers needs a logged-in editor or administrator to open a page or link that an attacker prepared, so the exposure is the set of accounts with edit rights to Event Gallery and what those people browse while they are logged in.

- Review who has edit permission for Event Gallery and remove it from accounts that do not need it
- If no one uploads from the frontend, unpublish the frontend upload menu item
- Ask editors to log out of the site before browsing elsewhere, and not to open unexpected links to the upload page
- Compare the images in your shop events against your originals if anything looks different, and run a full site audit
- Plan the Joomla upgrade that 6.5.0 needs, because none of this replaces the update

If you find images you did not upload, or anything else on the site you cannot account for, our Joomla hacked-site guide covers the order of work.

What we would like from Event Gallery's release notes

The fixes are good ones. A form token on the upload, an allow-list for the Back link target, random identifiers from `random_bytes()` and permission checks on every

backend action are the textbook answers, and the notes explain each change more clearly than most vendors manage. What is missing is a heading and a sentence.

Put the security entries under their own heading, above the features. Say which versions are affected, what an attacker could do in one line each, and that sites should update now. A CVE would put the release in front of every scanner at no cost to the vendor. None of that means publishing how to exploit anything. Until then, the safest way to read an Event Gallery release is to expand More information and search the page for “token”. If you look after more than a few Joomla sites, mySites.guru will tell you which ones need the update the morning it goes out.

Further Reading

- Event Gallery Core 6.5.0 release page - the full release notes, behind the More information button
- Event Gallery downloads - every Core release back to 3.x
- Twenty rules for Joomla extension developers handling a security report - what a security release should tell the people installing it
- OWASP Cross-Site Request Forgery Prevention Cheat Sheet - why a form token is the standard defence
- CWE-352: Cross-Site Request Forgery, CWE-79: Cross-site Scripting and CWE-330: Use of Insufficiently Random Values - the three weakness classes behind the 6.5.0 fixes

Frequently Asked Questions

Is Event Gallery 6.5.0 a security release?

Yes. Eight of the 46 entries under Bug Fixes in the 6.5.0 release notes are security fixes: a missing form token on the image upload, a reflected XSS on the frontend upload page, guessable cart and order identifiers, and missing token or permission checks on several backend actions. Update every site to 6.5.0.

Is there a CVE for the Event Gallery 6.5.0 fixes?

Not at the time of writing. We found no CVE, advisory or vulnerability database entry for any of them. The vendor fixed the issues itself, and we did not find or report them, so we do not know whether a CVE has been requested.

Can the Event Gallery upload CSRF be used to take over a Joomla site?

Not on its own. Before 6.5.0 a page on another website could make a logged-in editor upload an image into an event, or replace one with the same name, but uploads are still limited to jpg, gif, png, webp and mp4 files whose content matches an allowed image or video type. It lets an attacker change what a gallery shows, not run code on the server.

Does Event Gallery Core have the upload flaw, or only Extended?

Both. The frontend upload page only renders its uploader in Extended, but the upload task that was missing the token check exists in the Core component's backend and frontend controllers. The mySites.guru rule flags the component, which Core and Extended both install.

Why can my Joomla site not install Event Gallery 6.5.0?

Event Gallery 6.5.0 is published for Joomla 5.4 and later and for Joomla 6. On the day it came out, about a third of the connected Joomla sites below 6.5.0 were still running Joomla 3, and a further 7% were on Joomla 4. Those sites need a Joomla upgrade before they can take the fix.

Do old Event Gallery orders stay guessable after updating?

Yes. The vendor's notes say carts and orders created before 6.5.0 keep the identifier they already have, so links to them keep working. Only new carts and orders get the random identifiers. The vendor also says order download links were always protected by a separate random token.

How do I find every site running an old Event Gallery version?

mySites.guru records the version of every extension on every connected Joomla site twice a day. Its Joomla vulnerability database flags every Event Gallery component below 6.5.0, so every affected site shows the warning on its dashboard and in its audit.

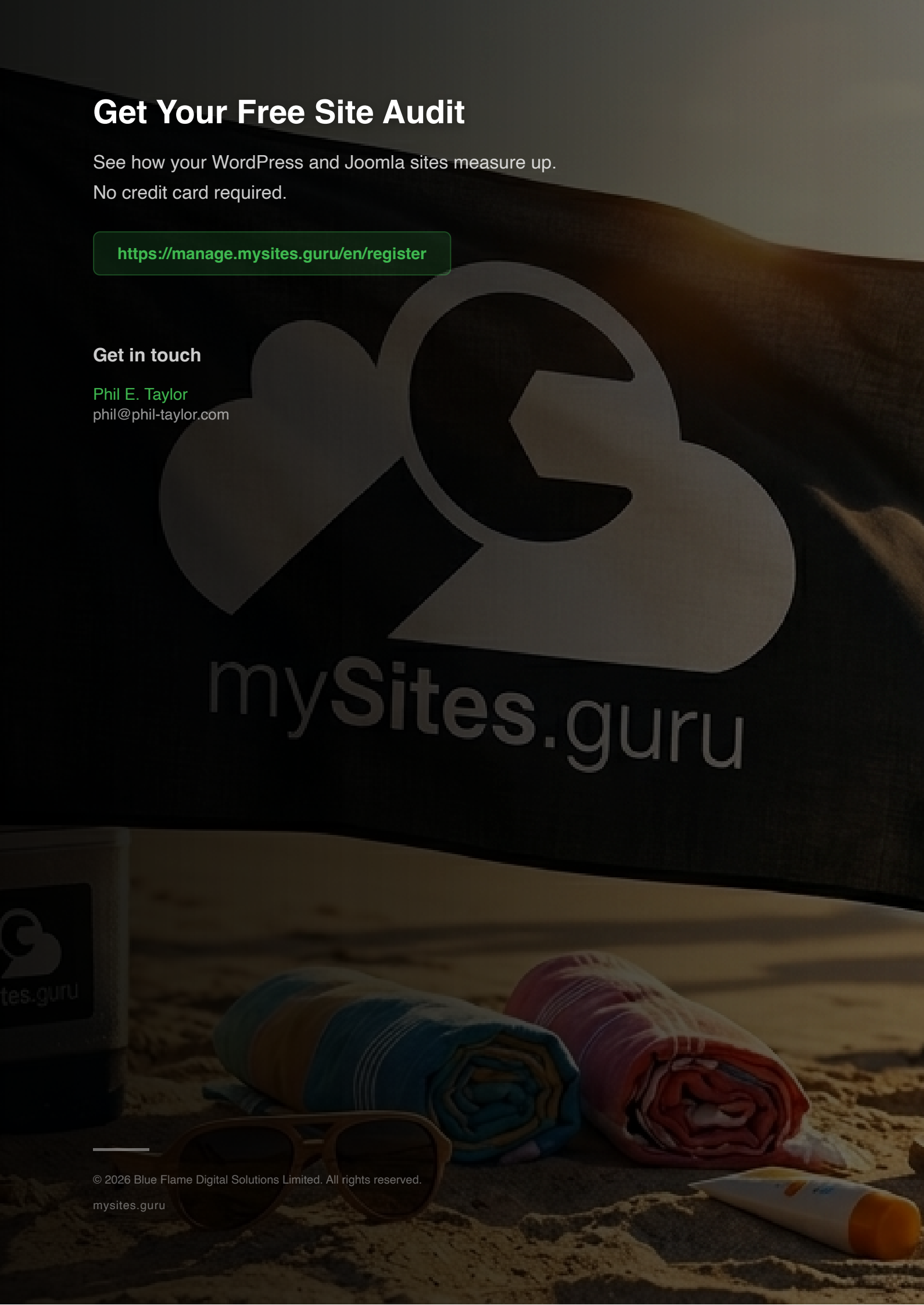
Written and edited by a human, with AI assistance. Our approach to AI

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