mySites.guru

Gantry 5.6.7 Fixes a File Picker Upload Flaw, but Not on Joomla 3 or 4

Gantry 5.6.7 hardens the Joomla file picker that let module managers upload any file type. Update Joomla 5 and 6 sites. Joomla 3 and 4 have no fixed release.

Phil E. Taylor | 4 November 2026

TL;DR

Gantry 5.6.7 was released on Wednesday 4 November 2026 for WordPress, Joomla and Grav. The vendor calls it “a security and stability release” that includes “a hardening of the Joomla file picker” and “a Grav compatibility fix”, and says “We recommend updating all sites on every platform”. The security fixes are in 5.6.6, released earlier the same day; 5.6.7 fixes a fatal error in 5.6.6, so 5.6.7 is the one to install. Before the fix, a Joomla backend user with only Modules manager rights could upload a file of any type, including PHP, through Gantry’s file picker.

Joomla 5 and Joomla 6 sites can install 5.6.7 today. Joomla 3 and Joomla 4 sites cannot: the 5.6.7 installer requires Joomla 5.0.0 or later, and the last Gantry 5 releases for Joomla 3 (5.5.19) and Joomla 4 (5.5.25) still contain the old file picker code. A little over a third of the Gantry 5 sites we monitor run Joomla 3 or 4.

8.6
CVSS 4.0

Gantry 5 file picker upload (no CVE assigned)

HIGH

mySites.guru assessment, from the Gantry 5.5.25 and 5.6.6 source

A backend user with only Modules manager rights could upload any file type through Gantry's file picker.

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

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N`	Network: Reachable across the internet
`AC:L`	Low: Nothing to work around, it just works
`AT:N`	None: Works against any affected install
`PR:H`	High: Needs an account with elevated rights
`UI:N`	None: Nobody has to be tricked into anything

What it does to the site

`VC:H` High: Everything the site holds can be read

`VI:H` High: Data and files can be altered at will

`VA:H` High: The site can be taken down

What it does beyond the site

`SC:N` None: Other systems keep their data

`SI:N` None: Other systems keep their integrity

`SA:N` None: Other systems stay up

No fix for Joomla 3 or 4

Gantry 5.6.7 installs on Joomla 5.0.0 and later only. Gantry 5.5.19 is the last release for Joomla 3 and 5.5.25 the last for Joomla 4, and both still have the unfixed file picker. The only full fix for those sites is Joomla 5.

What Gantry 5.6.6 and 5.6.7 Fix in Joomla

Two Gantry releases went out on 4 November 2026. Gantry 5.6.6 is the security release, published on GitHub at 16:37 UTC. Gantry 5.6.7 followed at 22:14 UTC and adds one line to the changelog: “Fixed a fatal error on some platforms when checking whether detailed error pages may be shown.” There was no public 5.6.5; its security commit was folded into 5.6.6. Install 5.6.7, which has the security fixes and the fix for the fatal error.

The 5.6.6 changelog lists the security changes under Common and Joomla. The Common entries are “Security: hardened permission checks and input handling in the admin file picker”, “Security: hardened validation of archive contents during outline import”, “File picker uploads are now limited to images, SVG, fonts and common video formats, with file type verification” and “File picker paths are limited to the site’s media and image folders”.

The Joomla entries are “Users who can only manage modules can still pick and upload images in the particle module editor, but have no other file picker access” and “File picker uploads respect the Media Manager’s allowed file extensions”. The first Joomla

line describes the access module managers used to have by stating what they are now limited to.

The Joomla File Picker Let Module Managers Upload Anything

Gantry 5 is a template framework, a Joomla extension, and its admin component has its own file picker for choosing and uploading images and other assets for particles. In the Gantry 5.5.19 and 5.5.25 source, the admin entry point `administrator/components/com_gantry5/gantry5.php` lets a user with `core.manage` on `com_modules` into every Gantry admin request as long as the request has `format=json`. The comment in the code says this was so the particle module editor could make its AJAX calls.

```
// administrator/components/com_gantry5/gantry5.php (Gantry 5.5.25)
&& !($user->authorise('core.manage', 'com_modules') && strtolower($app->in

// Filepicker.php (Gantry 5.5.25), upload function
// TODO: check if download is of supported type.
```

In the same versions, the file picker's upload function has the comment `// TODO: check if download is of supported type.` and then moves the uploaded file to the target path without any file type check. The picker's path "chroot" was `str_replace('..', '', $drive)`. Put the two together and a backend user who can manage modules, but has no access to Gantry or to Templates, could upload a file of any type, including PHP, through Gantry's file picker. The vendor has not said this was exploited, and we have not seen it exploited either. 5.6.6 closes the gap.

A Super User or a Templates manager can already change template code, so the file picker gave them nothing new. The exposure is the lower-privileged Modules manager. Modules manager rights are the kind of access a site owner gives a content editor so they can change a banner or a sidebar, on the understanding that it does not reach the template or the server. On a Gantry site below 5.6.6, it did. The same shape, an

authenticated upload with no type check that ends in code execution, is what we wrote up in Phoca Download, and 5.6.6 fixes it the usual way: uploads limited to images, SVG, fonts and common video formats with file type verification, respecting the Media Manager's allowed extensions, and module managers held to picking and uploading images in the particle module editor only.

Outline Import and the Debug Error Page

5.6.6 also has two smaller fixes. Outline import, the archive upload in the Gantry admin, did not reject archive entries with `..` segments or absolute paths before 5.6.6; it does now. This one needs Gantry admin access, so the audience is a Gantry or Templates manager rather than a module manager, and the hardened validation of archive contents is what the changelog refers to.

The third change was folded into 5.6.6 from an unreleased 5.6.5 commit. A particle AJAX request with an invalid outline could show the detailed Whoops debug error page to a visitor who was not an administrator. The vendor's WordPress readme calls it "a sensitive data exposure issue" and describes it for unauthenticated requests on WordPress; the error page condition change is in shared code. After the fix the debug page shows only in debug mode or to administrators, and secret values on it (passwords, keys, tokens, salts, database values, cookies) are masked.

Which Joomla Sites Can Install the Fix?

Only Joomla 5 and Joomla 6 sites can install Gantry 5.6.7. The installer in the Joomla package requires Joomla 5.0.0 or later and PHP 8.1 or later. Gantry 5.5.19 is the last Gantry 5 for Joomla 3 and 5.5.25 is the last for Joomla 4, and both still contain the file picker code above. There is no fixed Gantry release for Joomla 3 or Joomla 4.

Joomla version	Last Gantry 5 for it	Has the fix?	What to do
Joomla 3	5.5.19	No	Mitigate below, then move to Joomla 5

Joomla version	Last Gantry 5 for it	Has the fix?	What to do
Joomla 4	5.5.25	No	Mitigate below, then move to Joomla 5
Joomla 5	5.6.7	Yes	Install 5.6.7
Joomla 6	5.6.7	Yes	Install 5.6.7

Even on Joomla 5 and 6 the Update tab may not show it yet. Gantry's live Joomla update feed, checked on 4 November 2026 at about 22:45 UTC, offers 5.5.19 to Joomla 3, 5.5.25 to Joomla 4 and 5.6.4 to Joomla 5 and 6. Neither 5.6.6 nor 5.6.7 was in the feed, so the Joomla Update screen will not offer them until Gantry updates it. Install the package from gantry.org/downloads or the GitHub release instead of waiting.

Across the Joomla sites we monitor with Gantry 5 on 4 November 2026, none had updated to 5.6.6 or above at the time of writing. 5.6.4 is the most common installed version, on nearly half of them. About a quarter run Joomla 3, and a little over a third run Joomla 3 or Joomla 4, so more than a third of the Gantry 5 sites we see cannot install this fix at all. Most extension security releases leave a site one update away from the fix. This one leaves a third of its Joomla sites on a Joomla version the vendor no longer builds for. Gantry's page on the Joomla 3 security hub and the hub's options page cover the position for Joomla 3 sites; we set out the broader cost of staying on Joomla 3 in our agency retainer post.

What To Do Now on Each Joomla Version

On Joomla 5 and Joomla 6:

1. Back up the site. The vendor's own advice is "Back up the site before updating".
2. Install Gantry 5.6.7, not 5.6.6, because 5.6.7 fixes the 5.6.6 fatal error. Take the package from gantry.org/downloads or the GitHub release if the Update tab does not offer it, or push it to every site through the mySites.guru mass updater once the feed catches up.

3. Confirm the version afterwards on the Gantry 5 component (com_gantry5) or the Gantry 5 package (pkg_gantry5).

On Joomla 3 and Joomla 4, where there is no fixed release:

1. Review which user groups have Modules manager access (the Manage permission, core.manage, on com_modules) in Joomla's permission settings, and remove it from anyone you would not trust with template code. On an unfixed Gantry site, the two are the same thing.
2. Check the site for PHP files outside the normal Joomla folders, and for administrator accounts you did not create. We covered how to find rogue admin accounts in Joomla separately.
3. Plan the move to Joomla 5. That is the real fix, because it is the only way to install the Gantry release that closes the file picker.

Find administrator accounts you never created

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 →

Find files that match known hacks

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 →

How mySites.guru Flags Gantry 5 Below 5.6.6 on Joomla

On 4 November 2026 we added a rule that flags every connected Joomla site running Gantry 5 below 5.6.6. It reads the versions of the Gantry 5 component (com_gantry5) and the Gantry 5 package (pkg_gantry5), so a site shows as affected whichever of the two the Joomla extensions list reports. Joomla 3 and 4 sites are flagged too, on purpose: the rule says whether the site has the flaw, not whether the vendor has a package for it, and an agency with a mixed set of Joomla versions needs the list of sites that cannot be updated more than the list that can.

The flag works the same way as every other entry in our vulnerable extension list, alongside the security release flag on extension updates. Every rule we hold is listed on the public vulnerabilities page, and all of it is part of the subscription.

Gantry After RocketTheme

Joomla 3 sites cannot get the fix because of a decision Gantry took over a year ago. Gantry 5.5.20 dropped Joomla 3.x support, announced on 17 July 2025 for release on 23 July, which is why 5.5.19 is the last version a Joomla 3 site can install. For Joomla 4, Gantry's update feed stops at 5.5.25. RocketTheme, Gantry's original developer, concluded in 2025 ("The RocketTheme mission officially concluded", its site states, as of 30 June 2025), and Gantry installs now report the developer as Tiger12, LLC, while older installs still say RocketTheme, LLC. The project is still releasing, including this security fix, but it is releasing for Joomla 5 and later only.



Joomla 3 Didn't Fail. Your Retainer Did.

We monitor 30,305 live Joomla 3 sites. They are five times more likely to be hacked than Joomla 6, and the agencies who migrated...

Read the full post →

If a site has already been hit, or you would rather someone else made sure, fix.mySites.guru patches the site, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Further Reading

- Gantry 5.6.7 has been released - the vendor's own announcement for WordPress, Joomla and Grav.
- Gantry 5.6.7 on GitHub - the release with the Joomla, WordPress and Grav packages.
- Gantry 5 CHANGELOG - the 5.6.6 and 5.6.7 entries this post quotes.
- Upcoming release: Gantry 5.5.20 - the July 2025 announcement that dropped Joomla 3 support.
- Gantry on joomla3security.com - the Joomla 3 security hub's vendor page.
- Joomla 3 End of Life and Agency Retainers - why unfixable extensions are the real cost of staying on Joomla 3.
- Phoca Download Authenticated File Upload RCE - another authenticated upload-to-code-execution flaw in a Joomla extension.

Frequently Asked Questions

What do Gantry 5.6.6 and 5.6.7 fix in Joomla?

5.6.6 holds the security fixes: hardened permission checks and input handling in the admin file picker, uploads limited to images, SVG, fonts and common video formats with file type verification, picker paths limited to the site's media and image folders, hardened validation of archive contents during outline import, and the debug error page no longer shown to non-administrators. 5.6.7, released later the same day, only fixes a fatal error in 5.6.6 on some platforms, so install 5.6.7.

Is there a CVE for the Gantry 5 file picker flaw?

No. The vendor gives no CVE, no CVSS score, no researcher credit and no first affected version, and says nothing about exploitation. The 8.6 High score in this post is our own CVSS 4.0 assessment, based on the 5.5.25 and 5.6.6 source.

Can Joomla 3 or Joomla 4 sites update Gantry to 5.6.7?

No. The Gantry 5.6.7 Joomla installer requires Joomla 5.0.0 or later and PHP 8.1 or later. The last Gantry 5 for Joomla 3 is 5.5.19 and the last for Joomla 4 is 5.5.25, and both still contain the unfixed file picker code. Until the site moves to Joomla 5, remove Modules manager rights from any user you would not trust with template code, and check the site for PHP files outside the normal Joomla folders and for administrator accounts you did not create.

Why does Joomla's Update tab not show Gantry 5.6.7 yet?

Because Gantry's live Joomla update feed had not been updated when we checked on 4 November 2026. It still offered 5.6.4 to Joomla 5 and 6 sites. Until Gantry updates the feed, download the package from gantry.org/downloads or the GitHub release and install the zip the way you would any other Joomla extension.

How do I check which Gantry version a Joomla site runs, and how does mySites.guru flag it?

Look at the version of the Gantry 5 component (com_gantry5) or the Gantry 5 package (pkg_gantry5) in the Joomla extensions list. mySites.guru reads both and flags every connected Joomla site running Gantry 5 below 5.6.6, including the Joomla 3 and 4 sites that cannot install the fix.



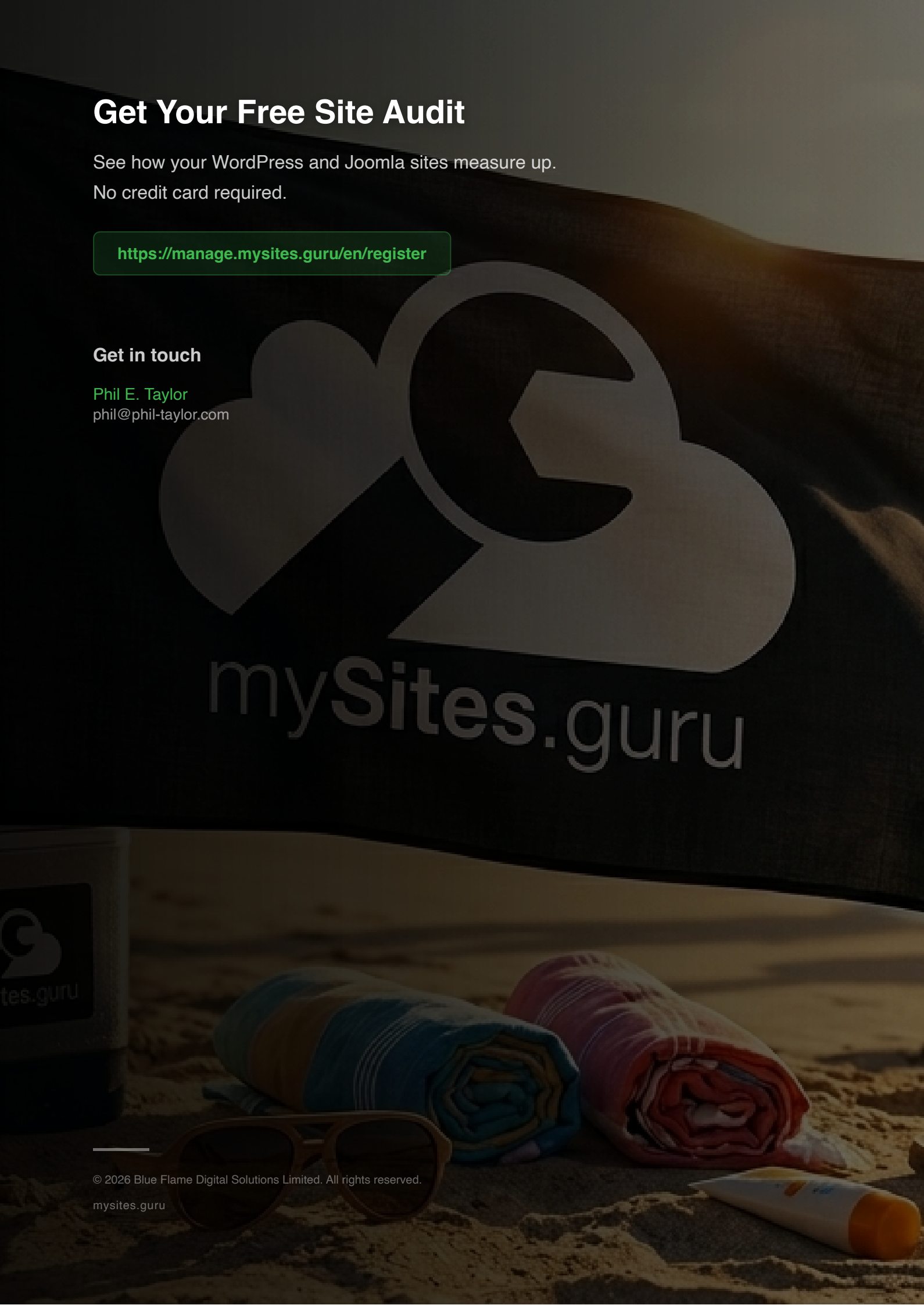
Written and edited by a human, with AI assistance. Our approach to AI

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.