mySites.guru

JoomShaper Patched the Joomla 3 It Said It Never Would

Six days after ruling out Joomla 3 security patches, JoomShaper shipped them for Helix Ultimate, Helix3 and SP Page Builder. What is in them.

Phil E. Taylor | 27 August 2026

Six days ago, JoomShaper told everyone still running Joomla 3 exactly where they stood. The announcement listed what Joomla 3 users could expect from the company, and the third bullet was the one that mattered: “No security patches, regardless of severity.”

Today, JoomShaper released security patches for Joomla 3. Helix Ultimate, Helix3 and SP Page Builder, all three of them, for the version of Joomla the company had just finished writing off.

That is the right call, and it arrived quickly. It is also a straight reversal of a position that was six days old, and if you manage Joomla 3 sites it changes what you should do this week. So we downloaded the packages and read the code rather than the announcement.

What JoomShaper Shipped for Joomla 3

Three separate patches, released today:

Product	Joomla 3 patch	Where it lives
Helix Ultimate	Security fixes v1.0.0, patching the plugin to a `2.1.4-j3sec` baseline	GitHub release tag
Helix3	Security patch v1.0.0, plugin and template to 3.1.2	GitHub release tag
SP Page Builder	The existing manual patch, now installable through Joomla	JoomShaper site download

The SP Page Builder entry comes with an admission worth reading twice. JoomShaper says it “released the SP Page Builder security update for Joomla 3 a while back, but it had to be applied manually”, and today’s release just makes that same patch installable through the extension installer. So a Joomla 3 security patch for SP Page Builder already existed at the point the company announced there would be no Joomla 3 security patches, regardless of severity.

These are security-only releases. JoomShaper is explicit that no other bug fixes are included, and the rest of the 9 July position has not moved: no new features, no bug fixes, no technical support, and migrate as soon as you can. The security-patch line is the part that changed.

What To Do About It Today

If you run Joomla 3 sites with any of these three extensions on them, the job this week is short: work out which sites are affected, get the patch onto them, and then check whether anything got in during the window when they were open.

The first part is the part that does not scale by hand. mySites.guru keeps a live inventory of every Joomla and WordPress site in your account with the core version and full extension list for each, so you can filter for Joomla 3 sites, search for Helix or SP Page Builder, and see the real list rather than guessing from memory. It flags end-of-life versions automatically too, so the exposed sites surface on their own.

See which of your sites this actually affects

Open your Extension Inventory

Filter for Joomla 3 and search for Helix or SP Page Builder. Not a subscriber? Sign up free and connect your sites.

The second part is where the vendor route gets tedious. Look at what JoomShaper's own instructions actually ask of you: download three separate zip files from three different places, two GitHub release tags and a site download, then log into every single Joomla site you manage and upload each patch by hand through the extension installer. For one site that is a coffee break. For forty Joomla 3 sites with a mix of these three extensions on them, it is a day you were not planning to spend, and it is the kind of job where site thirty-seven gets skipped and nobody notices until something else does.

The day before this reversal, we shipped our own tool that backports JoomShaper's fixes into the Joomla 3 builds, because at that point the vendor had said the fixes were

never coming. They have now come, and we are not going to pretend that is bad news: a vendor patch is better than a third-party guard, and if the official patch installs cleanly on your site, take it. What our toolset saves you is the legwork. One toggle applies the fix logic for every affected JoomShaper product across every site in your account at once, with a backup taken first and a one-click revert, instead of three downloads and forty logins.

What neither route changes is the gap people keep walking into. Patching closes the door. It does not evict whoever is already inside.

What Is Actually in the Patch

We read the code, and the fixes are real ones rather than cosmetic hardening. The Helix3 AJAX plugin is the clearest example, because it is the entry point behind CVE-2026-49049, the flaw we disclosed and the doorway for the AntonKill defacement wave.

The patched plugin now runs a deny-by-default allowlist. Every action is checked against a list of permitted names before anything happens, and anything unrecognised is rejected. The write actions, `save`, `remove`, `load`, `resetLayout`, `import`, `updateFonts` and `fontVariants`, now go through a single gate that demands both a valid CSRF token and real administrator permission:

```
private function requireAuthorisedAdminRequest()
{
  $user = $this->getCurrentUser();

  if ($user->guest || (!$user->authorise('core.admin') && !$user->authoris
    $this->sendJsonError(Text::_('JERROR_ALERTNOAUTHOR'), 403);
  }

  if (!Session::checkToken('request')) {
    $this->sendJsonError(Text::_('JINVALID_TOKEN'), 403);
```

```
    }
}
```

That is the correct fix. The original flaw was an anonymous visitor reaching those actions with no token and no permission check at all, and this closes it at the right point.

The rest is the same standard applied consistently. Layout filenames are sanitised down to alphanumerics, hyphens and underscores, then resolved with `realpath()` and confirmed to sit inside the layout directory, which kills the traversal. Image uploads are restricted to an extension allowlist. Raw `$_POST` access is replaced with Joomla's input filter. Imports and layout saves are capped at 1MB. The public voting action gets a token and a rate limit of five votes a minute.

Helix Ultimate gets the same treatment across a wider surface: an open redirect fix on the `helixreturn` login flow, central token and permission enforcement on the AJAX actions, upload hardening, and output escaping through the mega menu. Every menu field, the title, anchor attributes, icon and image classes, is now run through `htmlspecialchars()`, with dedicated sanitisers for badge text and colours. That is the stored cross-site scripting hole in the site chrome being closed at the output end.

The Version Gate Nobody Mentions

> **Correction, 27 August 2026**
>
> This section originally said the installer declares a supported range of 2.1.0 to 2.1.4-j3sec and rejects older builds, and it quoted a `SUPPORTED_HELIX_MIN` constant. That constant does not exist. We re-read the shipped `script.php` in the 1.0.0, 1.0.1 and 1.0.2 packages and there is no lower bound of any kind. Older 1.1.x and 2.0.x builds install fine. If you skipped a site in July because of what we wrote here, that site can take the vendor patch and should get it. The section below is rewritten to describe what the installer actually does.

The announcement does not mention this, and it still matters for anyone planning a patching round.

The Helix Ultimate Joomla 3 patch checks what you are running before it will touch anything, but only at the top end. Its installer declares a single supported ceiling:

```
const HELIX_BASELINE = '2.1.4-j3sec';
const SUPPORTED_HELIX_MAX = '2.1.4-j3sec';
```

The only version test is `version_compare($helixVersion, self::SUPPORTED_HELIX_MAX, '>')`, so the install aborts with "Unsupported Helix Ultimate version" when you are running something newer than the Joomla 3 baseline, and proceeds on everything at or below it. In practice that means 1.0.x, 1.1.x, 2.0.x, 2.1.0 through 2.1.3 and the patched 2.1.4-j3sec itself are all accepted. Plain 2.1.4 and the 2.2.x line are refused, which is the point of the gate: those are Joomla 4 and 5 builds that have no business on a Joomla 3 site.

It also requires Joomla 3.10.x specifically and PHP 7.2.5 or later, and it will not run if the Helix Ultimate system plugin is not installed at all.

So the practical answer for an old Joomla 3 site is better than we first reported. Check the version you are actually running rather than the version you assume, but expect the vendor patch to install even on a site that has been sitting on a 1.1.x build for years. Migration is still the real fix; the patch is a stopgap you can now apply almost everywhere.

The Logistics Are Rough

Three practical things we hit trying to follow JoomShaper's own instructions, which you will hit too.

The download links are missing. Both the Helix Ultimate and Helix3 sections tell you to "Download the security patch .zip file from GitHub" and neither sentence is a link. The packages exist and they are properly built, with checksums and a self-uninstalling installer, but the announcement does not get you to them. They are on the `j3-security-v1.0.0` release tag of each repository, linked in the table above.

The SP Page Builder patch is somewhere else entirely. It is not on GitHub with the other two, because the SP Page Builder repository has not been touched since 2020. It comes from the JoomShaper site download instead.

And the patched extension does not announce itself. The Helix Ultimate package patches files to a `2.1.4-j3sec` baseline and then removes itself, so a patched site does not obviously look different from an unpatched one. If you are tracking this across a lot of sites, record what you patched as you go, because the version number is not going to tell you later.

Patching Is Not Cleaning

The reason this distinction matters more than usual: these particular flaws were exploited in the wild before any of these patches existed.

SP Page Builder's unauthenticated upload, CVE-2026-48908, was scored CVSS 10.0 and used to plant hidden Joomla Super Administrators. The Helix3 flaw fed a defacement wave that stores its payload in the database rather than in a file. The Helix Ultimate mega-menu issue was used to store cross-site scripting inside the menu settings, aimed at creating a Super User out of the next admin who logged in.

Every one of those leaves something behind that a patch does not touch. A rogue Super Administrator survives patching. A payload sitting in the `params` column of your `#__menu` table survives patching, and survives a file scan, and survives a clean-file restore, because it was never a file. Attackers plant dormant droppers, hidden admins and malicious cron jobs so that the obvious cleanup misses them.

So if a site of yours was running a vulnerable build while these holes were open, patch it and then check it. mySites.guru ships one-click cleanup tools for these exact artefacts: rogue Super Admin accounts flagged by the signatures these campaigns reuse, the poisoned Helix Ultimate mega menu, the Helix3 custom code hack, and the rogue SP Page Builder icon-font assets. They work whatever Joomla version the site runs, because this wave hit Joomla 4, 5 and 6 sites as well.

Does This Change the Migration Advice?

Not in the slightest, and JoomShaper says so itself in the patch notes.

Joomla 3 reached end of life in August 2023. The paid eLTS programme that extended it ended in February 2025. Since then the core has had no official security patches of any severity, and today's release does nothing about that, because it patches extensions, not the platform they sit on. A hardened extension on an unpatched core is a better position than an unhardened one. It is still not a supported site.

What today buys you is breathing room, and the right use of breathing room is to spend it migrating. The targets are Joomla 5 or Joomla 6. Not Joomla 4: its own security support ended in October 2025, so migrating 3 to 4 moves you onto another unsupported line. For the core itself in the meantime, mySites.guru applies the backported Joomla 3.10.999 security patches with a single toggle, which closes the known core holes while you plan the move.

The Bottom Line

JoomShaper got to the right answer, and got there in six days. That deserves saying, because the alternative, a vendor leaving a CVSS 10.0 class of flaw unpatched on the majority of live Joomla sites, was a bad outcome and it did not happen.

What the six days show is how much weight a vendor's end-of-life policy holds when it is announced as final. For the length of that window, every agency running Joomla 3 was told the fixes were never coming and made decisions on that basis. Some of those decisions were "leave it, nothing can be done". The patches were reachable enough that they shipped less than a week later.

The practical takeaway is the same one we keep arriving at. Know which sites you have, know what is on them, patch what you can, clean what got hit, and keep migrating. Start with a free audit on one site if you want to see what your Joomla 3 exposure actually looks like.

Further Reading

- JoomShaper: Security Update for Joomla 3 Users - today's announcement and the patch notes for all three products.
- JoomShaper: Joomla 3 Support Has Come to an End - the 9 July announcement, including the "no security patches, regardless of severity" line.
- Helix Ultimate j3-security-v1.0.0 release - the actual packages, checksums and fix list.
- Helix3 j3-security-v1.0.0 release - the Helix3 plugin and template patches.
- CVE-2026-48908 - the SP Page Builder unauthenticated upload record, CVSS 10.0.
- CVE-2026-49049 - the Helix3 unauthenticated write record behind the AntonKill wave.
- Joomla End of Life dates - which Joomla versions are still supported.

Frequently Asked Questions

Did JoomShaper reverse its Joomla 3 decision?

On the security patches, yes. On 9 July 2026 JoomShaper said Joomla 3 builds of its products would get no security patches, regardless of severity. On 15 July 2026 it released security patches for the Joomla 3 builds of Helix Ultimate, Helix3 and SP Page Builder. The rest of the 9 July position stands: no new features, no bug fixes, no technical support, and Joomla 3 is still end of life. What changed is the security-patch line specifically.

How do I install the JoomShaper Joomla 3 security patch?

Helix Ultimate and Helix3 patches are on GitHub, on the j3-security-v1.0.0 release tag of each repository. JoomShaper's own announcement tells you to download the zip from GitHub but the link is missing from the page, so go to the release tag directly. The SP Page Builder Joomla 3 patch is not on GitHub at all and comes from the JoomShaper site download instead. Each one installs through Joomla's normal Install Extensions screen, and the Helix Ultimate package removes itself afterwards.

Will the JoomShaper Joomla 3 patch install on my site?

Probably, yes. Correction, 27 August 2026: we originally wrote that the Helix Ultimate Joomla 3 patch only supports Helix 2.1.0 to 2.1.3 and refuses older builds. That was wrong. Re-reading the installer, the only version gate is an upper bound: it refuses anything above 2.1.4-j3sec and has no lower bound at all, so the 1.1.x and 2.0.x builds still common on long-lived Joomla 3 sites are accepted. It does require Joomla 3.10.x and PHP 7.2.5 or later, and it refuses the Joomla 4 and 5 builds of Helix, which is the gate we misread.

Does the patch change my extension version number?

The Helix Ultimate Joomla 3 package patches the plugin files to a 2.1.4-j3sec baseline rather than shipping a normal version bump, then uninstalls itself. So the extension is hardened in place. This matters if you track versions across a lot of sites, because a patched site does not necessarily look different from an unpatched one at a glance.

Does this mean I can stay on Joomla 3 now?

No. Migration to Joomla 5 or 6 is still the only real fix, and JoomShaper says the same thing in its own patch notes. Joomla 3 reached end of life in August 2023 and the paid eLTS programme that extended it ended in February 2025. A patched extension on an unpatched

core is a safer holding position, not a supported one. Treat this as breathing room to plan the migration, not a reason to cancel it.

Does patching clean a site that was already hacked?

No, and this is the part people get wrong. A patch closes the entry point so it cannot be used again. It does not remove anything an attacker planted while the hole was open, such as a hidden Super Administrator or a payload stored in the database rather than in a file. If a site was exposed during the window, patch it and then check it for what got in. mySites.guru has separate one-click cleanup tools for exactly those artefacts.

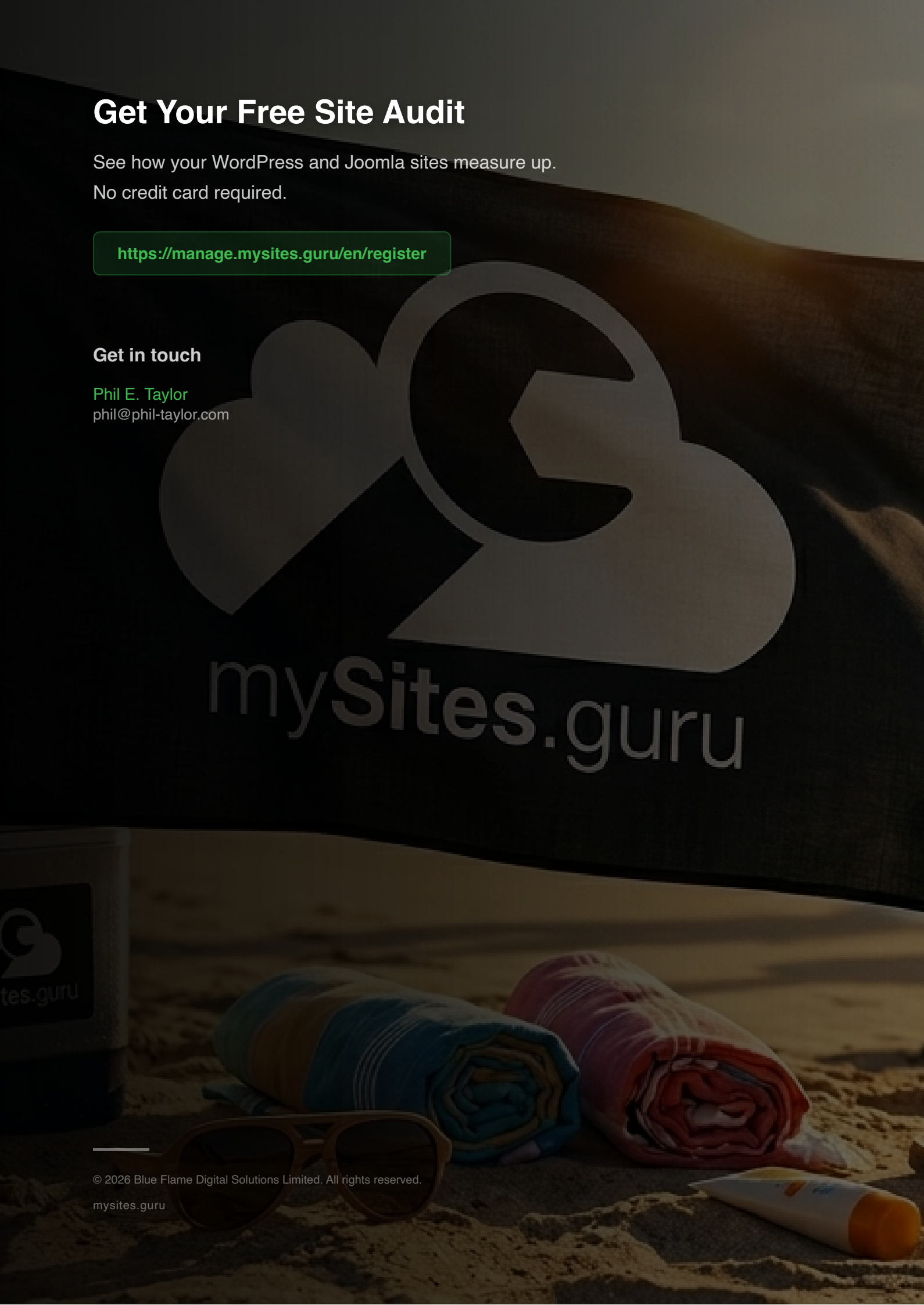
Written and edited by a human, with AI assistance. Our approach to AI

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.