Helix Ultimate's Third Joomla 3 Patch Since JoomShaper Said There Would Be None

JoomShaper said its Joomla 3 products would get no security patches regardless of severity. The Helix Ultimate template framework has now had three.

Phil E. Taylor | 27 August 2026

4+ LIVE **Joomla extension security alerts** (26 Aug) Sourcerer 16.0.0 · Fabrik 4.7.2 · ZOO: unauth RCE · JCE 2.9.99.10

TL;DR: JoomShaper published a third Joomla 3 security patch for the Helix Ultimate template framework on 27 August 2026, after announcing in July that its Joomla 3 products would receive “No security patches, regardless of severity.” The patch contains genuine fixes, including an access-control bypass reachable without logging in, and the company emailed customers the same day with a stated severity of High to Medium. This post is about the Joomla 3 package only. The problem with it is delivery: the patched system plugin and template both report version `2.1.4-j3sec`, the same string the July build reports, so Joomla’s updater will never offer them and no tool can tell a patched site from an unpatched one. The patch package also deletes its own extension record when it installs, leaving nothing behind for Joomla to check. Across the Joomla 3 sites we manage that run Helix Ultimate, roughly two thirds report that version string, and every one of them first reported it before this release existed.

On 9 July 2026 JoomShaper announced that the Joomla 3 builds of all its products were finished. One line did the damage: “No security patches, regardless of severity.” Six days later the company shipped Joomla 3 security patches anyway. A week after that it shipped another. Today it shipped a third.

> **“No security patches, regardless of severity.”**
>
> JOOMSHAPER, 9 JULY 2026. THREE JOOMLA 3 SECURITY PATCHES LATER.

Shipping the patches is the right call, and we have said so each time. Joomla 3 runs more than half the live Joomla web, and a vendor that keeps patching it despite saying it would not is doing its users a favour. But the third release has a problem the first two

did not, and it is the kind of problem that quietly undoes the patch: on Joomla 3, the fixed files report the same version number as the broken ones.

That matters because version numbers are how everything downstream decides whether you are safe. Joomla's updater compares them. Extension inventories record them. Our own scanner reads them off every site in your account. When the patched build and the vulnerable build both say `2.1.4-j3sec`, every one of those systems gives the same answer for both, and that answer is wrong half the time.

This is a Joomla 3 problem only. Sites on Joomla 4, 5 and 6 get the same security work through the normal Joomla updater, and we have covered that release separately. Everything below is about the Joomla 3 route.

What Does the Third Joomla 3 Patch Actually Fix?

These are not our findings. JoomShaper ran its own security pass on the Joomla 4 and 5 line, and this release backports that work into the Joomla 3 build. We did not discover or report any of it. What follows comes from reading the published code difference between the July and August releases, so we can tell customers what changed rather than take a changelog on trust.

The most serious item is an access-control bypass that needed no login at all. Before this release, adding `?helixMode=edit` to any URL on a Helix Ultimate site did two things for an anonymous visitor. It skipped the Coming Soon redirect entirely, so an unlaunched site was served in full to anyone who knew the parameter. And it made the framework load template settings from the draft cache instead of the saved ones, so the visitor saw the administrator's unsaved work-in-progress design. Both now require an account with template edit rights.

The rest is real but narrower:

- **Mega menu writes are now scoped to one menu.** The `saveMegaMenuSettings` endpoint checked only that you could edit menus somewhere. Anyone who passed

that check could rewrite the mega menu settings of any menu item on the site. It now checks permission against the specific menu the item belongs to.

- **Media path resolution got proper canonicalisation.** The old check cleaned the path and compared it as a string against the allowed roots. String comparison does not follow symlinks, so a symlink inside the images folder pointing elsewhere passed the test. The new code resolves the real path first and rejects null bytes.
- **Image uploads are now decoded, not just named.** Uploads are checked with `getimagesize`, `finfo` and a full decode, instead of trusting the file extension.
- **The Page Title feature escapes its output.** Heading tags come from an allowlist, background colours must match a hex pattern, and the background image URL is quoted and escaped before it reaches the `style` attribute.

That is a decent list, and the release notes describe it honestly. JoomShaper also emailed customers the same day with a stated severity of High to Medium and told Joomla 3 users to download this package and install it by hand, which is the correct instruction and more communication than most Joomla extension vendors manage.

The Helix Ultimate Version Number Did Not Change, But the Code Did

We flagged the shape of this in July, when the first Joomla 3 patch went out. That post warned that the 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, and told people to write down what they patched because the version number would not tell them later. What has changed is that it has now happened three times. The same string covers three different payloads, so it can no longer separate a patched site from an unpatched one, or one patch round from another.

The August release ships three files. One is the patch package, `helixultimate_j3_security_fixes_v1.0.2.zip`, which went from 1.0.1 to 1.0.2 as you would expect. The other two are the framework itself: the system plugin and the

starter template. Both of those are still called `2.1.4-j3sec`, which is what the July release called them.

The contents are different. We downloaded both releases, unpacked the system plugin from each, and compared the trees:

```
$ diff -rq jul/plg_system_helixultimate aug/plg_system_helixultimate
Files .../src/Platform/Blog.php differ
Files .../src/Platform/Helper.php differ
Files .../src/Platform/Media.php differ
Files .../src/HttpResponse/Response.php differ
Files .../src/fields/helixmegamenu.php differ
Files .../layout/megaMenu/container.php differ
...
118 differences in total
```

Both of those packages declare `2.1.4-j3sec`. One of them has the access-control bypass fixed and one does not, and nothing on the site can tell you which you have.

A smaller oddity from the same check, offered as an observation rather than an accusation: the three files attached to the July release do not match the `SHA256SUMS` published alongside them. The August release verifies cleanly. The likeliest explanation is that the checksum file was generated from a different build of the same source than the one uploaded, which is the sort of thing that happens when a release is assembled quickly.

> **Important**
>
> A version number is a promise that the same string means the same code. When a vendor breaks that promise on a security release, every automated check downstream inherits the mistake, including ours. Reusing a version string on changed files is worse than not shipping a fix, because it makes an unpatched site look patched.

How Many Joomla 3 Sites Are Affected?

We track every extension and its version on every Joomla and WordPress site in our customers' accounts, which is how we can answer this rather than guess at it.

Across the Joomla 3 sites we manage that run the Helix Ultimate system plugin, roughly two thirds report version `2.1.4-j3sec`. The remaining third are spread across older builds, mostly the 1.1 and 2.0 lines, and some of those go back years.

Then we checked when each of those sites first reported that version string. Every one of them reported it before the August release went out. Not one site in the accounts we monitor has picked up the new build, which is unsurprising a few hours after publication. But it is the whole problem in one line: two thirds of the affected sites are advertising the version number of the fixed build while running the code of the broken one.

Why Will Joomla Never Offer This Update?

Three separate things stop the update reaching a site, and they compound.

The version number is identical. Joomla's updater asks whether the available version is newer than the installed one. `2.1.4-j3sec` is not newer than `2.1.4-j3sec`, so the answer is no, forever.

The update feed still points at July. JoomShaper's update feed has three entries. The patch package entry was correctly bumped to 1.0.2 today. The system plugin and template entries were not touched: both still declare `2.1.4-j3sec` and both still link to the `j3-security-v1.0.0` download from July. A site that does poll the feed is offered the old file.

The patch package deletes itself. This is the one that surprised us. The installer's `postflight` method ends by calling `uninstallPackage()`, which removes the package's own row from Joomla's extensions table. The design intent is clear enough: apply the fixes, leave no permanent extension behind. The side effect is that Joomla loses the extension record and the update site along with it, so there is nothing left to check for a 1.0.2.

Across every site in every account we monitor, the `helixultimatej3securityfixes` package has never once been recorded as installed. Not on the sites that plainly did apply it, which are sitting there reporting `2.1.4-j3sec`. The package works exactly as designed and erases the evidence that it ran.

That also means the advice in JoomShaper's own July release notes cannot work. The 1.0.1 notes tell users to go to Extensions, then Manage, then Update. For the package those notes describe, there is nothing in that list to update.

Today's customer email gets this right, and tells Joomla 3 users to download the ZIP and install it by hand instead. That is the correct instruction. It is also the only one that can work, which is the part the email does not explain.

The Second Joomla 3 Patch Advertised a File It Did Not Serve

The July round has its own version of this problem, visible in the same feed.

From 22 July to 27 August, the feed declared version `1.0.1` for the patch package while the download URL underneath pointed at `helixultimate_j3_security_fixes_v1.0.0.zip`. The 1.0.1 package existed and was attached to the GitHub release. The feed just never pointed at it.

For five weeks, any site that was offered that update and took it downloaded the 14 July build. Joomla would have installed it, recorded version 1.0.0 from the manifest, and offered 1.0.1 again on the next check. Today's release fixed the URL as a side effect of bumping it to 1.0.2, so the 1.0.1 package was effectively never distributed through the channel built to distribute it.

What the Helix Ultimate Patch Leaves Unfinished

We read the whole difference. Four things stop short of what the changelog claims.

The image removal endpoint now checks that you are allowed to edit an article before it deletes a file. It takes the article ID from the request, and never checks that the file being deleted has anything to do with that article. An author who owns one article can pass that article's ID along with the path to any image under the site's media folders, and the check passes. The authorisation is real, but it is guarding the wrong thing.

The Page Title fix escapes its background image URL twice, once into a cleaned variable and again on the way out. Any legitimate image URL containing an ampersand comes out mangled. It is a cosmetic bug rather than a security one, but it is a sign of how quickly this went out.

The same background image pattern the Page Title feature just fixed is still there, unescaped, in the template's main `index.php`, where the body background and reading progress bar settings go straight into a stylesheet declaration. Those values can only be set by someone who can already edit template settings, so the risk is low. It does mean the escaping work was a spot fix on one file rather than a sweep across the framework.

Finally, the release adds a `saveLicenseInfo` function to the framework's helper class, with a changelog bullet describing it as a security fix and a test asserting that its source code mentions the right database table. Nothing in the codebase calls it. It is dead code with a test that checks its spelling.

The July Flaws Did Get CVEs. This Round Has None Yet.

When we wrote about Helix Ultimate 2.2.7 in July we said no CVE had been assigned. That has since changed, and we have updated that post.

The Joomla CNA assigned two numbers on 13 July 2026:

- CVE-2026-57829, unauthenticated stored XSS in Helix Ultimate below 2.2.7. CVSS 4.0 base score 8.7, High.
- CVE-2026-57830, unauthenticated arbitrary file deletion in Helix Ultimate below 2.2.7. CVSS 4.0 base score 8.8, High. NVD scored the same flaw 9.1 Critical under

CVSS 3.1.

Nothing has been assigned for the August round. We would read that as the paperwork not having caught up rather than a judgement on severity, and numbers can still be assigned later by a researcher or by the Joomla CNA. No CVE today is not the same as no CVE ever.

Fifteen CVEs have been published against JoomShaper products, and eleven of them arrived in July and August 2026 alone, across SP Page Builder, EasyStore and Helix Ultimate. This is a vendor under sustained security scrutiny, doing a lot of remedial work at speed. The speed is showing in the delivery.

What Should You Do With Your Joomla 3 Helix Ultimate Sites?

Start by finding them, because most people underestimate how many they have. Every Joomla 3 site running the Helix Ultimate system plugin or the `shaper_helixultimate` template needs this, and the sites most likely to be running it are the ones nobody has logged into for two years.

Then apply the current patch, whatever the version number says. Because you cannot tell from the outside whether a site has the August build, the safe assumption is that it does not. Download `helixultimate_j3_security_fixes_v1.0.2.zip` from the release, verify it against the published SHA256SUMS file, and install it through Extensions, then Install. Re-applying it to a site that already has the fixes is harmless.

One change since the first Joomla 3 patch is worth knowing. That release refused to install on older Helix builds, which left a lot of 1.1.x and 2.0.x sites with no vendor option at all. The current installer only rejects versions *above* `2.1.4-j3sec` and no longer enforces a lower bound, so older builds that were turned away in July will now accept it.

After patching, check the site rather than assume. The access-control bypass exposed unlaunched sites and draft settings, and the mega menu write reached menus the user

had no business touching. Look at your Joomla Users list for Super User accounts you do not recognise, review your mega menu and template settings for entries you did not add, and check your media folders for files you did not put there.

Doing This Across an Account

If you look after more than a handful of Joomla sites, the finding part is the expensive bit, and it is what mySites.guru is for. Search for Helix Ultimate once in your mySites.guru account and you get every site running it, the version each one reports, and the Joomla version underneath, without logging into anything. That is the same inventory the figures earlier in this post came from.

For Joomla 3 sites specifically, mySites.guru has a one-click patch for the abandoned JoomShaper extensions. The **Unpatched JoomShaper Security Holes** toggle in the **Hacked?** section of a site's Snapshot applies the fix logic in place, across Helix Ultimate, Helix3 and SP Page Builder, on every site in your account rather than one at a time. It takes a backup of the original files first, so switching it off restores them.

Neither of those makes Joomla 3 supported again. Migration is still the only real answer, and everything here is a way of holding a site safely while you get budget and sign-off for the move. If a Joomla 3 site has already been compromised, patching will not clean it: fix.mysites.guru handles that for a single fixed fee of GBP 120 per incident, usually same day, and we screen the site before committing so you are not charged in the rare case it cannot be fixed.

The Bottom Line

JoomShaper said it would ship no Joomla 3 security patches regardless of severity, and has now shipped three. That is the right outcome, arrived at awkwardly, and the code in this one is real work that closes a bypass anyone on the internet could have used.

The delivery undermines it. A security fix that ships under the version number of the flaw it fixes cannot be detected, cannot be offered by the updater, and cannot be audited across a portfolio. Every Joomla 3 site running this framework reports a number

that means two different things, and the only way to resolve the ambiguity is to patch it again and know for certain.

If you manage Joomla sites for clients, find every Helix Ultimate install you look after and treat all of them as unpatched. Start with a free audit on one site to see what your Joomla 3 exposure actually looks like.

Timeline

2026-07-09

JoomShaper says Joomla 3 will get no security patches

The announcement ends support for the Joomla 3 builds of every JoomShaper product, with one line doing the damage: no security patches, regardless of severity.

2026-07-15

The first Joomla 3 patch, six days later

J3 Security Fixes 1.0.0 ships for Helix Ultimate, alongside Joomla 3 patches for Helix3 and SP Page Builder. The stated policy lasted under a week.

2026-07-22

The second patch, advertised but not delivered

J3 Security Fixes 1.0.1 is released. The update feed declares version 1.0.1 while the download link still points at the 1.0.0 file, and it stays that way for five weeks.

2026-08-27

The third patch, under the old version number

J3 Security Fixes 1.0.2 backports hardening from Helix Ultimate 2.2.10. The patched plugin and template files change, but both keep the version string 2.1.4-j3sec that the July build already used.

Further Reading

- Helix Ultimate J3 Security Fixes v1.0.2 - the Joomla 3 release itself, with JoomShaper's changelog and the download packages.
- Helix Ultimate 2.2.10 - the same security work for Joomla 4, 5 and 6, which updates in the normal way.
- CVE-2026-57830 - the unauthenticated arbitrary file deletion in Helix Ultimate below 2.2.7, assigned by the Joomla CNA in July.
- CVE-2026-57829 - the unauthenticated stored XSS from the same round.
- Joomla 3.10 end of life - the official notice, and the reason none of this has a supported core underneath it.

Frequently Asked Questions

What is Helix Ultimate J3 Security Fixes 1.0.2?

It is the third Joomla 3 security patch JoomShaper has released for the Helix Ultimate template framework, published on GitHub on 27 August 2026. It backports JoomShaper's mainline security hardening into the Joomla 3 build: an access-control bypass that let anonymous visitors past a Coming Soon page and into draft template settings, a mega menu write that was not scoped to a single menu, a symlink escape in media path handling, stricter image upload validation, and output escaping in the Page Title feature.

How do I tell whether a Joomla 3 site already has the August fixes?

By version number, you cannot. The patched system plugin and template both report 2.1.4-j3sec, which is the same version string the July build reports, even though the files inside changed. Joomla's Extensions manager, the update feed and every inventory tool see the same number either way. The only reliable answers are to compare the plugin files against the published release, or to apply the current patch again so you know what is on disk.

Will Joomla offer me this update automatically?

Not on Joomla 3. The patch package removes its own extension record from Joomla as the last step of installation, so a site patched in July has nothing left for the updater to check and no update site to poll. The plugin and template entries in JoomShaper's update feed still declare version 2.1.4-j3sec and still point at the July download, so even a site that does poll is offered nothing new. JoomShaper's own customer email tells Joomla 3 users to download the ZIP from GitHub and install it manually, which is the only route that works. Joomla 4, 5 and 6 sites are different: they get Helix Ultimate 2.2.10 through the normal Joomla updater.

Did mySites.guru report these flaws?

No. This was JoomShaper's own security pass, backported from its Joomla 4 and 5 line. We did not discover or report any of it. We read the published code difference between the July and August releases so we could tell customers what changed and which sites are affected, which is a different thing from finding the flaws.

Is there a CVE for this release?

Not at the time of writing. The July round did get numbers: CVE-2026-57829 and CVE-2026-57830 were assigned by the Joomla CNA on 13 July 2026 for the unauthenticated stored XSS and arbitrary file deletion in Helix Ultimate below 2.2.7. Nothing has been

assigned for this August round yet. That is paperwork catching up rather than a verdict on severity, and a researcher or the Joomla CNA can still assign numbers later.

Which Joomla 3 sites need this?

Any Joomla 3 site running the Helix Ultimate system plugin or the shaper_helixultimate template. The installer refuses anything above 2.1.4-j3sec and no longer enforces a lower bound, so older 1.1.x and 2.0.x builds that the first Joomla 3 patch turned away will now accept it.

Does patching remove a compromise that already happened?

No. Patching closes the way in. If a site was reachable through the access-control bypass or the media path flaw, anything already changed on it stays changed. After patching, check the Joomla Users list for Super User accounts you do not recognise, review mega menu and template settings for entries you did not add, and confirm your media folders hold only files you expect.

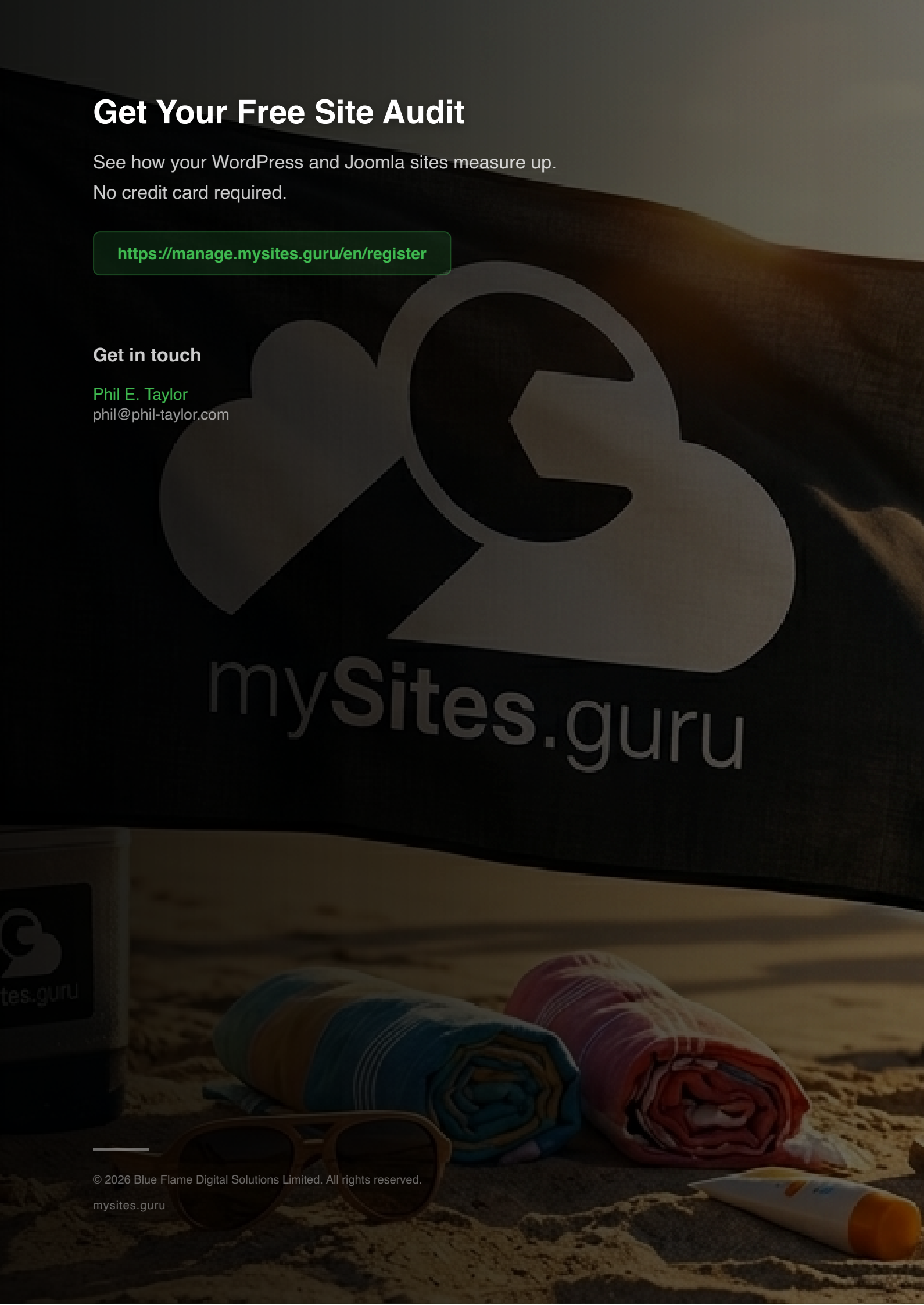
Written and edited by a human, with AI assistance. Our approach to AI

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