The One-Click Way to Patch JoomShaper Extensions on Joomla 3

mySites.guru backports JoomShaper's security fixes into SP Page Builder, Helix3 and Helix Ultimate on Joomla 3, in place and across every site in your account, from one toggle.

Phil E. Taylor | 15 July 2026

Update, 15 July 2026: JoomShaper has now patched Joomla 3

The day after this post went out, JoomShaper reversed its position and released Joomla 3 security patches for Helix Ultimate, Helix3 and SP Page Builder. That is good news and worth taking: if the official patch installs on your site, apply it. Two things to know first. The Helix Ultimate package only supports Helix 2.1.0 to 2.1.3 and refuses older builds, and no patch, ours or theirs, cleans up a site that was already breached. **We read the patch code and wrote up what is in it**.

There are still thousands of Joomla 3 sites out there.

There is always a reason, an excuse: a client who will not sign off the budget, a custom template nobody has the source for, a booking system that only exists as a Joomla 3 extension. So the sites sit there, end of life, and you keep an eye on them and hope. Pray. Ignore.

On 9 July 2026, JoomShaper stopped supporting Joomla 3 across every one of its products, with one line that matters more than the rest: **no security patches, regardless of severity.**

In the same fortnight, we found and disclosed twelve separate vulnerabilities in popular Joomla extensions, four of them rated the maximum CVSS 10.0

Unfortunatly, attackers weaponised the fixes within hours of each one going public, as is the norm nowadays.

JoomShaper only fixed their own code running on Joomla 4+ and left those with Joomla 3 sites scrambling around without any security fixes.

So we built the tool that fixes NOT ONLY the hacks from their vulnerabilities - but also PATCHES their extensions/plugins that they abandoned in their time of need.

mySites.guru now patches the abandoned JoomShaper extensions on Joomla 3, SP Page Builder, Helix3 and Helix Ultimate, in place, and cleans up the sites already hit, all from the same dashboard you use to manage everything else.

BUILT BY MYSITES.GURU

This tool backports JoomShaper's own security fix logic into the Joomla 3 extension code you are actually running, in place and reversibly, across every site in your account from one toggle. We wrote it, we tested it against real vulnerable sites for a week, and it is live in your subscribed account now (GBP19.99 per month - unlimited sites!). It is one of several Joomla 3 tools we have shipped in the last few weeks, because the sites that need them are the ones with nobody else left to help.

JoomShaper Walked Away From Joomla 3. Like many modern developers.

You cant blame them. Joomla 3.x.x has been end of life for years. mySites.guru already has a tool that patches security issues in Joomla 3.10.12 following the end of life announcement by Joomla, and their failed commercial eLTS support service - which also ended.

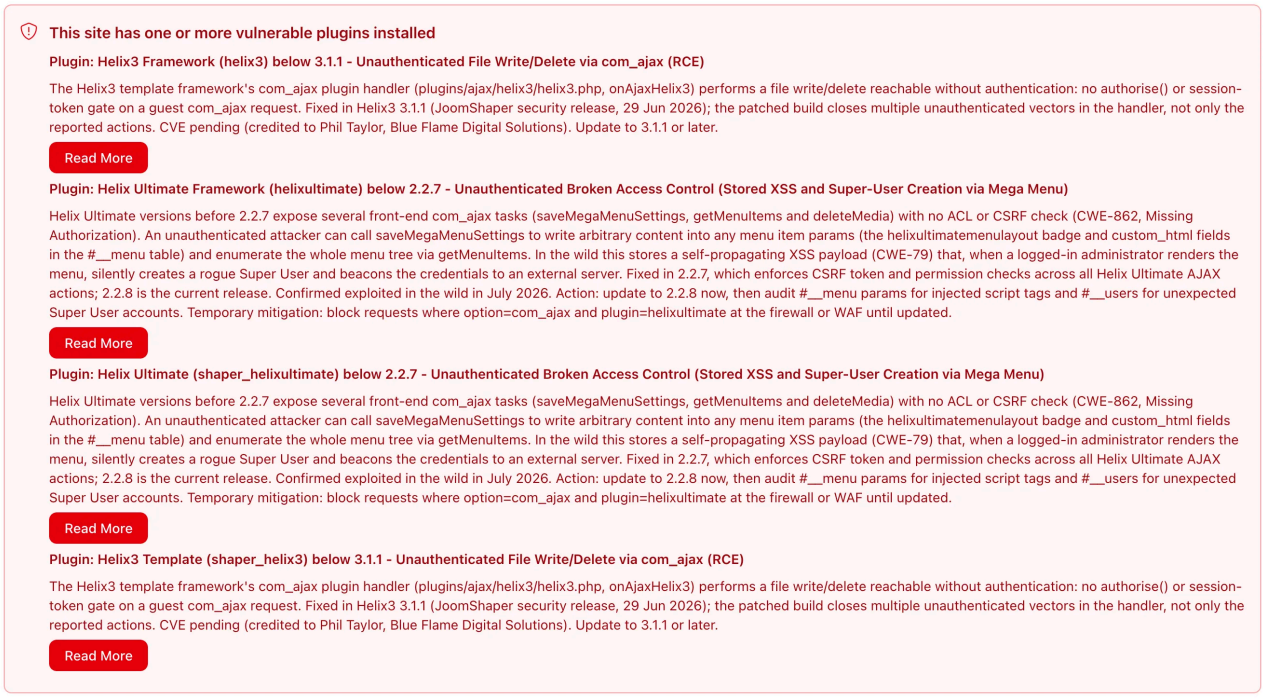
JoomShaper's decision is defensible, and we said so at the time: it can secure its own code, but it cannot secure the end-of-life Joomla core underneath it. The timing is what makes it bite. SP Page Builder had an unauthenticated file-upload flaw, CVE-2026-48908, rated CVSS 10.0 and actively exploited to plant hidden Joomla Super Admins. Helix3 had CVE-2026-49049, the entry point for the "Hacked by AntonKill" defacement wave that hides its payload in your database, not your files.

Both are patched, and when we built this tool both official fixes existed only for Joomla 4 and above.

- The fix for SP Page Builder is version 6.6.2.
- The fix for Helix3 is 3.1.1,
- and for Helix Ultimate it is 2.2.7.

Every one of those requires Joomla 4 or newer. Run them on Joomla 3 and there is no version you can update to.

On 15 July 2026, the day after this tool shipped, JoomShaper reversed its Joomla 3 decision and released separate Joomla 3 patches for all three products. If one installs on your site, take it: a vendor patch beats a third-party guard. The catch is that the Helix Ultimate package checks your version first and only supports Helix 2.1.0 to 2.1.3, so the older builds that tend to sit on long-lived Joomla 3 sites are refused outright.



mySites.guru already spots these on every connected site and tells you exactly which flaw is present, which version fixes it and why it matters, so before you patch anything you can see your real exposure as a list instead of finding out from a defacement.

These are the JoomShaper vulnerabilities we have found, disclosed and written up, the three products this tool patches on Joomla 3:

JoomShaper extension	Vulnerability	CVE	Severity	Read
SP Page Builder	Unauthenticated icon upload to RCE	CVE-2026-48908	10.0	Read
Helix3	Unauthenticated file write and delete via com_ajax	CVE-2026-49049	7.5	Disclosure and AntonKill wave
Helix Ultimate	Unauthenticated menu write to stored XSS	none assigned	High	Read

We took a different view. The fix logic that JoomShaper wrote is public, we have read it, and it is not large. So mySites.guru now applies that same logic directly to the Joomla 3 code you are running, without touching the version and without waiting. At the time we built it the vendor had said no. It has since said yes, which we are glad about, and the tool still saves you doing it by hand on every site.

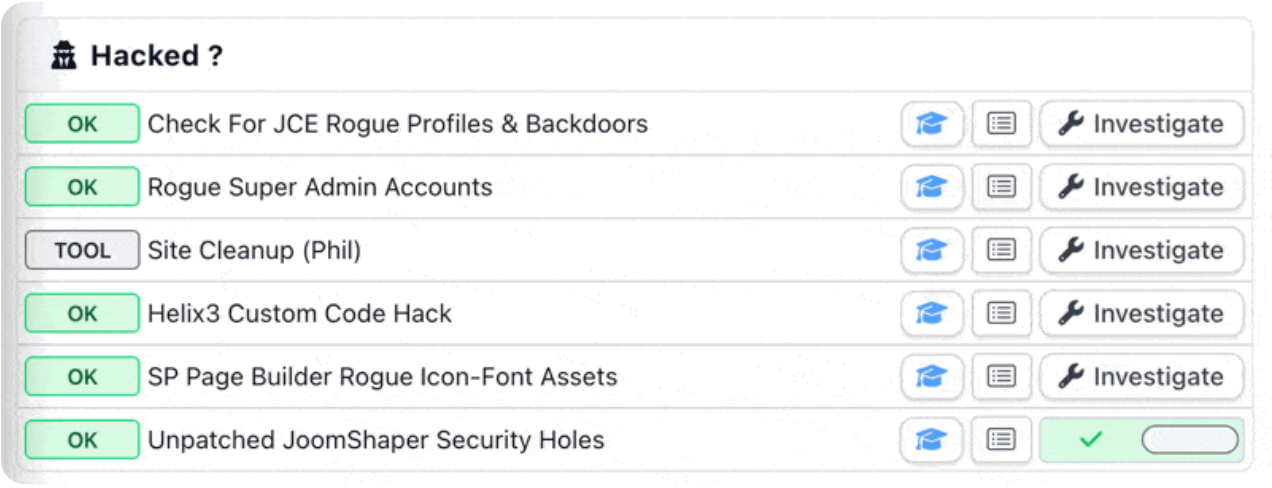
How to Patch JoomShaper Extensions on Joomla 3

With mySites.guru tools! A simple toggle in the site's Snapshot, in the same **Hacked?** section as our other security checks.

One click to patch, one click to restore original files.

Simple.

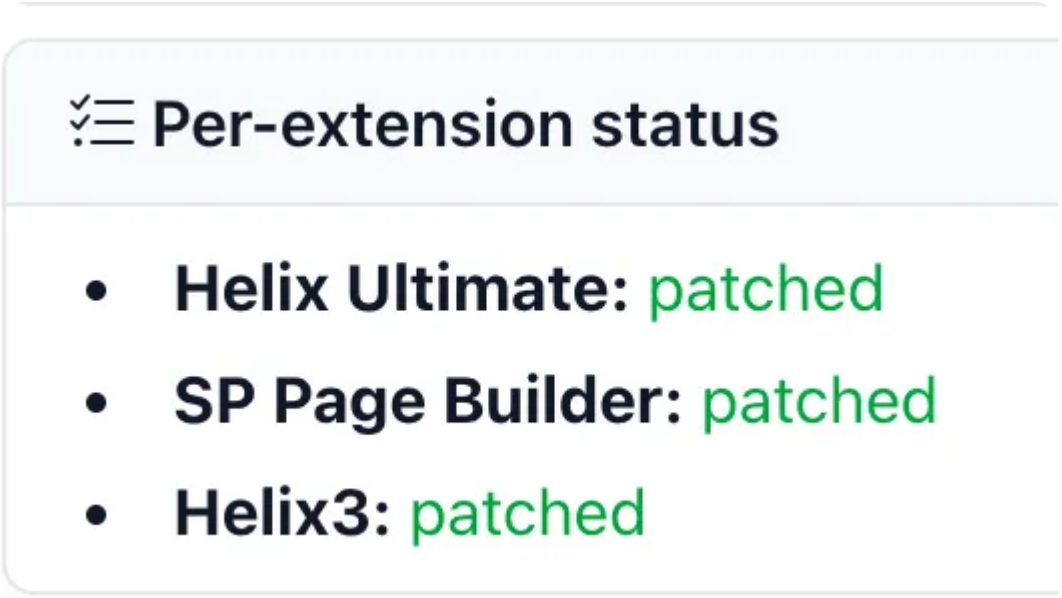
To patch JoomShaper extensions on a Joomla 3 site with mySites.guru, you flip a single toggle in the site's Snapshot, in the same **Hacked?** section as our other security checks. Flip it on and mySites.guru inspects the three abandoned JoomShaper extensions, works out which are present and still vulnerable, and injects a minimal security guard into each one through the connector. Flip it off and it restores the original files from the backup it took before the first change.



It is a guard, not a version bump.

Rather than trying to ship a rebuilt copy of every version of every extension anyone might be running, the tool reads the file, confirms the vulnerable code is actually there, and inserts a small, self-contained check at the exact point the vendor added theirs. That one approach covers the whole range of vulnerable versions instead of needing a hand-built file for each. Each guard is a faithful backport of the real fix:

- **Helix Ultimate**: the media handler that let an anonymous visitor delete files now requires an authenticated template editor and rejects any path containing `..`, the same gate JoomShaper added.
- **Helix3**: the AJAX image upload and remove handlers now demand a valid token and the right permission before they will do anything, closing the unauthenticated write.
- **SP Page Builder**: the addon parameter that could be steered into loading an arbitrary file is now restricted to a plain slug, which kills the local-file-include that led to remote code execution.



Once the toggle is on, the Snapshot shows a per-extension status so you can confirm at a glance which of the three JoomShaper extensions the guard closed on that site.

> The patch **does not change the extension's version number**, because it does not replace the extension. The vulnerability badge on the site stays visible on purpose, as a standing reminder that the only permanent fix is migration. What changes is that the hole is now closed.

Because it works across every site in your account, you are not logging into 400 admin panels to do this. You see every Joomla 3 site that runs a vulnerable JoomShaper extension in one list, and you patch them together. The backup-first, toggle-to-revert design means that if anything about a particular site makes you cautious, undoing the change is one click and leaves the files byte-for-byte as they were.

That is the difference worth understanding now that the vendor patches exist. Doing it JoomShaper's way means downloading three separate zip files from three different places, then logging into every Joomla site you manage and uploading each one by hand through the extension installer. Doing it this way is one toggle that applies the fix logic for every affected JoomShaper product across every site at once. Both close the same holes. Only one of them costs you a day.

What About the Joomla 3 Sites That Just Need to Hang On?

This tool exists precisely for them. Not every Joomla 3 site can migrate this quarter, and telling an agency to “just move to Joomla 6” ignores the real work involved: template rebuilds, extension replacements, content checks, client approval. In the meantime those sites are live, indexed, and exposed. The honest position is that they need to hang on for a while, and hanging on should not mean hanging out with an open door.

Alongside the JoomShaper patch, mySites.guru already includes a one-click patch for the Joomla 3 core itself. That tool applies every known Joomla 3 core security fix, backported from the 3.10.999 project and the eLTS work, across all your sites from a single toggle, no eLTS subscription required. Between the two, the core holes and the abandoned-extension holes on a Joomla 3 site are both closed while you plan the move properly.

Cleaning Up After the Hack Wave

Prevention is only half the story, because a lot of these sites were breached before anyone shipped a fix. The wave of Joomla hacks running through 2026 has defaced and backdoored sites in their tens of thousands, and the same JoomShaper flaws are the doorway for a good share of them. Joomla 3 sites are the worst exposed, because they cannot take the vendor fix, but the wave hit Joomla 4, 5 and 6 sites too, and these cleanup tools work on the affected sites whatever version they run. Once an attacker is in, they plant things designed to survive your cleanup: dormant droppers, hidden admins and malicious cron jobs that quietly rebuild the malware after you think you have removed it. So mySites.guru ships targeted, one-click tools for the exact artefacts these attacks leave behind.

mySites.guru has a full suite of tools that you can use to clean your hacked sites - the specific ones developed for this current wave are:

🔧 NEW TOOL: Remove Rogue Super Admin Accounts

The first thing a SP Page Builder or Helix compromise usually does is create a hidden Joomla Super Administrator, so the attacker keeps a way back in even after you patch. The **Rogue Super Admin Accounts** tool flags Super Admins planted with the known attacker signatures, by email and by the worm usernames these campaigns reuse, and lets you delete them across every affected site in one action. A site with a rogue Super Admin is shown as hacked, in red, until it is gone.

🔧 NEW TOOL: Clean the Helix Ultimate Mega Menu Hack

The newest of these tools shipped the same day as this post. When an attacker abuses the unauthenticated Helix Ultimate menu write on a Joomla 4, 5 or 6 site, they store a payload in the mega-menu settings, stored cross-site scripting aimed at creating a Super User, hidden inside your menu.

On a compromised site we examined, the `params` column of the Home item in the `#__menu` table read like a normal Helix Ultimate menu layout, except that inside the `helixultimatemenulayout` value two fields, `badge` and `custom_html`, had each been overwritten with the same block of JavaScript. Trimmed down, it does this:

```
// #__menu -> params -> helixultimatemenulayout -> "badge" and "custom_htm
<s-cript>(function () {
  var C2  = 'https://xdxd.olybrdbtrknks.xyz';                    // attack
  var DEF = { login: 'admin_mori', email: 'memetkaan43@proton.me', gid: '8

  // poll /administrator/index.php every 30s for a logged-in admin session
  // then scrape the one-time CSRF token from the page,
  // POST com_users task=user.apply to create the Super User,
  // and beacon the working credentials back to the C2 router.
  // (working parts trimmed on purpose)

  checkAdmin();
  setInterval(checkAdmin, 30000);
})();</s-cript>
```

A few things make it nasty:

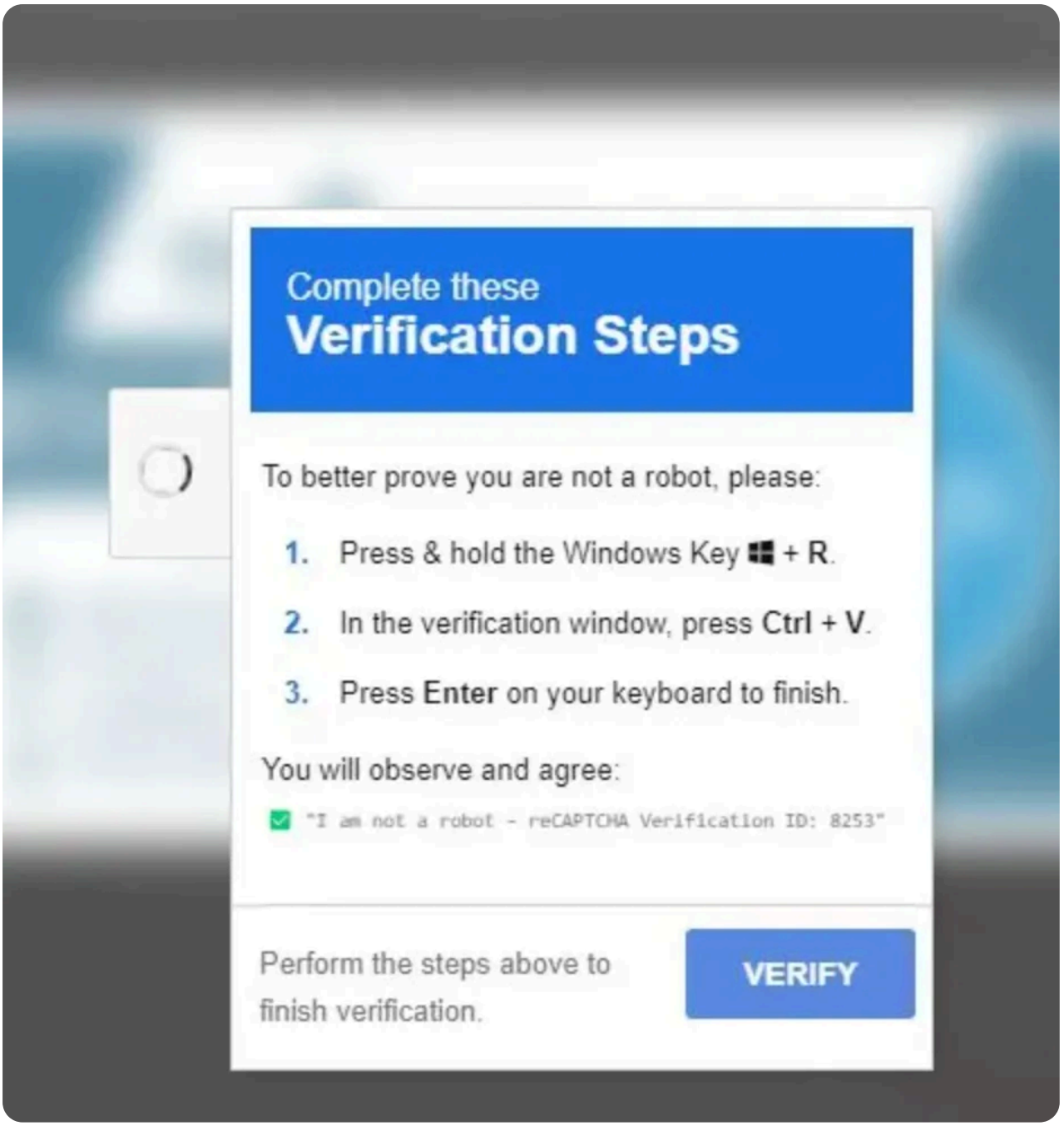
- **It lives in the database, not on disk.** File scanners, SFTP greps and clean-file restores all miss it, the same blind spot as the Helix3 defacement.
- **The tag is written as** `<s-cript>` (note the hyphen) so naive keyword filters skip over it, while the browser still parses it as a real script the moment the menu renders.
- **It only fires for a logged-in administrator.** The script quietly polls `/administrator/index.php` every 30 seconds, and as soon as it detects an authenticated admin session it submits the `com_users` new-user form on that admin's behalf, CSRF token and all.
- **The Super User is attacker-controlled.** Its username, password and email are fetched live from the C2, falling back to `admin_mori` / `memetkaan43@proton.me` in group 8 if the C2 is unreachable, then the working credentials are beaconed straight back so the attacker can log in from anywhere.

So the menu write is only the doorway. The real prize is a hidden Super User that outlives the patch, which is why cleaning the site means two jobs: blank the injected menu fields, and audit `#__users` for an admin account you did not create. **Indicators of compromise:** a `<s-cript>` string in `#__menu.params`; the C2 domain `xdxd.olybrdbtrknks.xyz`; a Super User named `admin_mori` or registered to `memetkaan43@proton.me`; a hidden iframe with id `jc_router_iframe`; the global flags `joomlacreater_inline_run` and `joomlacreater_create_done` in page source.

The **Helix Ultimate Mega Menu Hack** tool finds the poisoned menu items and blanks only the injected badge and custom-HTML fields, leaving the rest of your menu layout exactly as it was, then points you to update Helix Ultimate to 2.2.7 or later so it cannot happen again.

🔧 NEW TOOL: Clean the Helix3 Template Code Hack

The Helix3 version of the same attack hides its payload in the template style's custom code in the database, which is why an on-disk malware scan of a defaced Helix3 site comes back clean while the skull is still on the screen. The **Helix3 Custom Code Hack** tool reads every template style, finds the injected defacement or stealth loader, and clears it in one click. We wrote about where that defacement actually hides in detail.



The nastier variant does not deface at all. Instead of a skull, the stealth loader serves a fake “I’m not a robot” box like this one, a ClickFix lure that talks the visitor into pasting an attacker command into the Windows Run dialog and running it on their own machine. The homepage looks normal, the file scan is clean, and the site is quietly weaponised against everyone who visits it, which is exactly why a Helix3 site needs its template custom code checked whether or not a skull ever appeared.

🔧 NEW TOOL: Delete Rogue SP Page Builder Assets

The SP Page Builder upload flaw let anyone plant rogue icon-font asset rows as a foothold. The **SP Page Builder Rogue Icon-Font Assets** tool detects those planted rows and removes them, again across every affected site at once.

Find the Backdoors They Left on Disk

The database-side tools clean the specific artefacts these campaigns plant, but a breached site usually has files dropped through the same hole too, and those can be buried anywhere in tens of thousands of files. The mySites.guru file scanner flags each one as a **Hacked File**, so instead of grepping a whole web space by hand you get a short list to work through, and you can open any file to read the suspect content inline before you act on it.

That is a real dropper from one of these compromises: a small webshell that runs any command the attacker sends and lets them upload more files. It is the kind of thing that survives a database clean and re-infects the site later, which is why the file audit matters as much as the toggle.

Important

Patching and cleaning are two different jobs. Patch to close the entry point so it cannot happen again; clean to remove what an attacker already left. On a site that has been breached, do both, and run a full file audit afterwards, because these compromises rarely stop at one backdoor. If you would rather someone else handled it, our team fixes hacked Joomla sites for a flat fee at fix.mysites.guru.

Does Patching Let Me Skip the Joomla 3 Migration?

No. Migration to Joomla 5 or 6 is the only real fix, and none of these tools changes that. What they change is the risk you carry in the gap between now and the day that migration actually happens, which for most agencies is measured in months, not days. The patch tool closes the vendor-abandoned holes, the core patch tool closes the Joomla core holes, and the cleanup tools deal with anything that got in first. That is a defensible position to hold a site in while you do the migration properly, instead of leaving it open and hoping the botnets do not find it before you get to it.

If you manage more than a handful of Joomla sites, the starting point is knowing which ones are still on Joomla 3 and what each of them runs. mySites.guru inventories the extensions and versions on every Joomla site you connect and flags the end-of-life ones automatically, so your exposure is a list you can see rather than a surprise you find out about from a defacement.

A Joomla and WordPress Toolset That Grows Every Day

The Helix Ultimate mega-menu tool went into mySites.guru the day this post went out. The JoomShaper patch tool arrived the same week. The core Joomla 3 patch tool picks up new backports as new eLTS fixes appear. We shipped mySites.guru in 2012 and have not stopped building it since, and we mean that literally: we put work into it every single day of the year, because the threats change every single day of the year.

That investment runs across both platforms, not just Joomla. The same account that patches your Joomla 3 extensions also bulk-updates your WordPress plugins, scans

every site with malware detection built from over a decade of real hacks, backs everything up, and monitors for the changes that a second-wave attacker makes between two clean-looking scans. When a new CMS threat appears, we build the tool that fixes it across your whole portfolio and add it to the dashboard, usually within days, instead of just writing a knowledge-base article about it. The Joomla 3 tools in this post are simply the most recent proof of that.

Why Has the mySites.guru Price Not Changed Since 2012?

Because we decided a long time ago that the deal should get better without the price going up. mySites.guru is GBP 19.99 per month for unlimited Joomla and WordPress sites, and that number has not moved since we launched in 2012. Every tool in this post, the JoomShaper patch, the core Joomla 3 patch, all four cleanup tools, arrived after you signed up and cost you nothing extra. So did AI-powered malware analysis, the vulnerability alerting, and the hundreds of other things we have added over the years.

We are not aware of another service in this space that has held its price flat for that long while adding this much. When we build a tool like the only Joomla 3 extension patcher in existence, it does not become a paid add-on or a higher tier. It shows up in your account, at the price you already pay, because a toolset that grows every day is the entire point of paying for one. You can try the whole thing free for a month and see it for yourself.

Rather someone just fixed it for you? A flat GBP 120, even if the site is still on Joomla 3.

Please send me your complete site details, including FTP, using the form at **fix.mySites.guru** and I'll happily take a look. Set fees apply. Skip the troubleshooting and get your site fixed today.

Phil Taylor, the mySites.guru founder, has resolved thousands of Joomla and WordPress issues. Most fixes are completed within the hour, and at the latest the

same day.

✓ Same-day resolution guaranteed

✓ Fixed price, no surprises

✓ No fix? No fee!

Fix my site for GBP 120 →

Further Reading

- JoomShaper's announcement that it has dropped Joomla 3 support - the vendor's own statement, including the "no security patches, regardless of severity" line.
- CVE-2026-48908 on the NVD - the SP Page Builder unauthenticated file-upload flaw, rated CVSS 10.0.
- The Joomla 3.10.999 project on GitHub - the community-sourced backported core patches the core patch tool draws from.
- Joomla's official end-of-life policy - where Joomla 3 sits in the support timeline and why.

Frequently Asked Questions

How do I patch JoomShaper extensions (SP Page Builder or Helix) on a Joomla 3 site?

You flip one toggle. mySites.guru backports JoomShaper's own security fixes into the abandoned Joomla 3 builds of SP Page Builder, Helix3 and Helix Ultimate, applied in place as a minimal code guard through the connector. Turn on the Unpatched JoomShaper Security Holes toggle in the Hacked? section of the site's Snapshot and it patches whichever of the three vulnerable extensions are present. Flip it off and the original files are restored from the backup it took first.

Why can't I just update these extensions to the fixed version on Joomla 3?

The mainline fixed versions do not run on Joomla 3: SP Page Builder 6.6.2, Helix3 3.1.1 and Helix Ultimate 2.2.7 all require Joomla 4 or newer, so there is no version you can update to. On 15 July 2026, after saying it would issue no Joomla 3 security patches regardless of severity, JoomShaper reversed that and released separate Joomla 3 patches for all three products. Apply the vendor patch where it installs, but check your version first: the Helix Ultimate Joomla 3 package only supports Helix 2.1.0 to 2.1.3 and refuses anything older. Our tool applies the same fix logic in place, across every site in your account from one toggle, rather than site by site.

Does the patch tool clean a site that is already hacked?

No. The patch tool is prevention: it closes the entry point so an attacker cannot get in through these extensions again. If a site has already been breached, patching does not remove what the attacker left behind. That is what the cleanup tools are for. mySites.guru has separate one-click tools that remove rogue Super Admin accounts, blank the poisoned Helix mega-menu and Helix3 template code, and delete the rogue SP Page Builder assets planted through these exact flaws.

Is patching Joomla 3 a substitute for migrating to Joomla 5 or 6?

No, and we will not pretend otherwise. Migration is the only real fix. The patch tool is for the sites that genuinely cannot move yet, the ones that just need to hang on securely while you line up budget and sign-off. It buys you a safer window, it does not make Joomla 3 supported again.

Which JoomShaper extensions does the Joomla 3 patch tool cover?

Three: Helix Ultimate, SP Page Builder and Helix3, the JoomShaper products most likely to be sitting on an old Joomla 3 site and most likely to have produced a critical

unauthenticated flaw. The tool detects which of them are installed and vulnerable on each site and patches only those, leaving anything already up to date or absent untouched.

What does mySites.guru cost, and has the price changed?

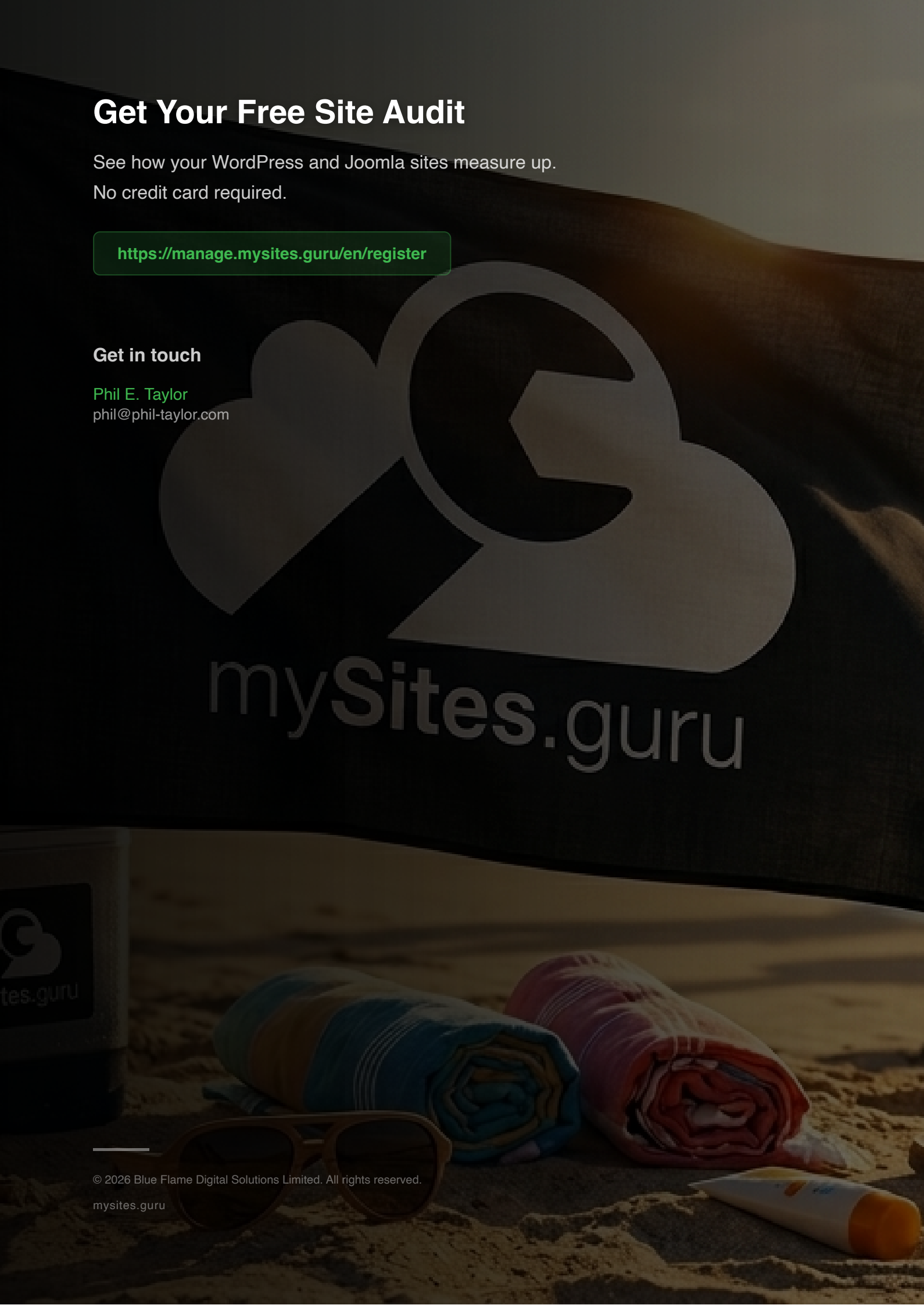
GBP 19.99 per month for unlimited Joomla and WordPress sites. That price has not changed since we launched in 2012, despite the fact that we add new tools like this one almost every week. You get every tool we have ever built and every tool we build next, for the same flat monthly price, with no per-site fees.

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