mySites.guru

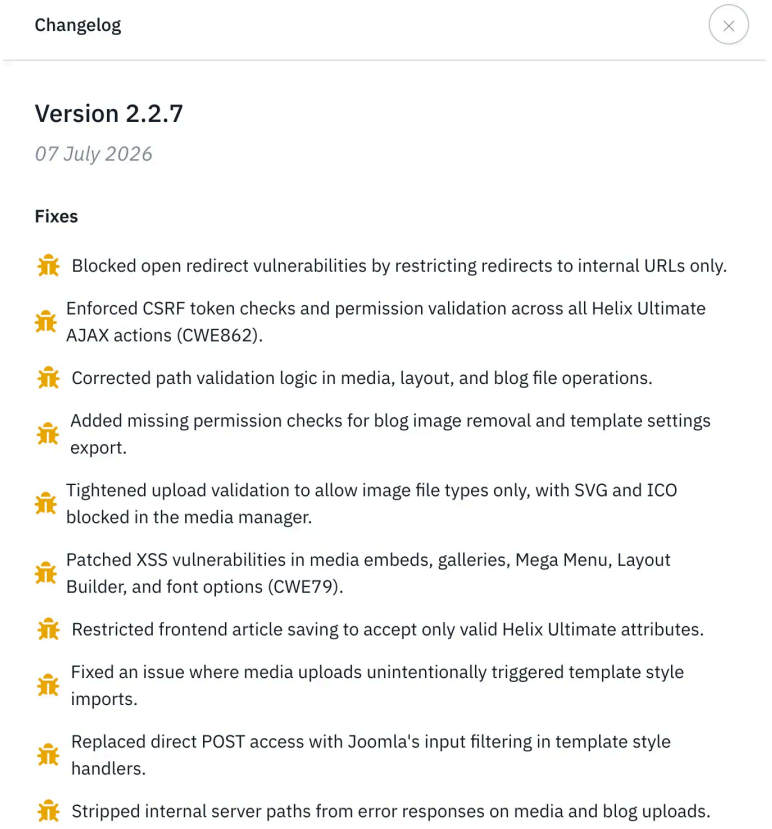
Helix Ultimate 2.2.7 Closes an Unauthenticated Menu Write

Helix Ultimate 2.2.7 quietly fixes CSRF and permission gaps in its com_ajax handler, an unauthenticated menu write that leads to stored XSS, an in-folder file delete, and an open redirect. Here is what changed and why to update today.

Phil E. Taylor | 7 July 2026

JoomShaper shipped Helix Ultimate 2.2.7 on 7 July 2026. It is a security release, and a substantial one: it puts missing login and permission checks back across the framework's AJAX handler, closes an unauthenticated write into your site's menus that leads to cross-site scripting, confines file operations so they cannot escape the folder they belong in, validates redirects, and tightens media uploads. None of that is obvious from the version number, and if you triage Joomla updates by how urgent they look, this one deserves to jump the queue.

To their credit, JoomShaper's in-app changelog for 2.2.7 does more than the usual two-word "Security Update". It lists the fixes and even tags them with the relevant weakness classes, CWE-862 for the missing authorisation and CWE-79 for the cross-site scripting:



That is genuinely better than most template vendors manage. What the changelog still does not tell you is how the flaws chained together, which one to worry about most, or how far behind your installed version really is. This post fills that in, so you can judge the severity for yourself and update with your eyes open.

TL;DR

TL;DR: Helix Ultimate 2.2.7 patches several security holes in the framework's `com_ajax` handler. Before the release, several AJAX actions ran with no CSRF token and no permission check, so an anonymous visitor could write to your menu settings, and because that output was not escaped, that is a route to stored cross-site scripting in your admin session. It also fixes an in-folder arbitrary file delete via a path-validation flaw, an open redirect through `helixreturn`, an unprotected template settings export, and loose media upload validation. Every version below 2.2.7 is affected; the last public release before it was 2.2.4 (22 January 2026). This is not a zero-day and there is no CVE, but the patched code is public. Update every Helix Ultimate site to 2.2.7 now. If you manage more than a handful of Joomla sites, mySites.guru can list every Helix Ultimate install in your account in seconds and push the update.

How to find every Helix Ultimate site you manage with mySites.guru

The first question after any framework security release is the awkward one: which of my sites actually run this? Helix Ultimate is one of the most widely installed template frameworks in the Joomla world, bundled under the bonnet of a large number of JoomShaper templates and plenty of third-party ones, so plenty of people are running it without ever having chosen it by name. A vendor's update notice only helps if you can connect it to the right sites.

mySites.guru keeps a live inventory of every extension, template and framework installed on every Joomla and WordPress site in your account. You search for Helix Ultimate once, and you get back every affected site, the version each one is running,

and whether the 2.2.7 update is available. No logging into 40 admin panels one at a time. No guessing.

View all your Helix Ultimate installations

Open your Extension Inventory

Search for Helix Ultimate across all your connected Joomla sites and filter for anything below 2.2.7 to find the installations that still need updating.

From that same list you can push the update to every affected site, so a vague sense of "I should probably check my sites" becomes a five-minute job across your whole account. If you are not a customer yet, run a free security audit on one site and see the extension inventory for yourself, or read how we manage multiple Joomla sites from one screen.

That is the practical answer. The rest of this post is the detail the changelog left out.

Helix Ultimate is not Helix3

JoomShaper ships two template frameworks with confusingly similar names, and they patched security holes in both within about a week of each other. Getting them mixed up will send you updating the wrong thing.

Helix Ultimate is the newer framework, and the subject of this post. It installs as the `helixultimate` system plugin plus the `shaper_helixultimate` template, and sometimes a small template installer plugin alongside them. Version 2.2.7 is the one you want.

Helix3 is the older, separate framework. It had its own set of unauthenticated file-write and file-delete flaws, fixed in Helix3 3.1.1 on 29 June 2026. That is a different codebase, a different version number, and a different update. If you run sites on both, each needs its own patch.

The vulnerable code in this case is Helix Ultimate's AJAX handler, reachable through Joomla's `com_ajax` dispatcher.

What the bugs actually did

Joomla has a built-in dispatcher called `com_ajax` that lets a plugin expose an endpoint at a predictable URL. It is a normal, useful feature. The catch, and it is the same catch behind a long line of Joomla extension bugs, is that `com_ajax` will happily call a plugin's handler for a completely anonymous visitor. Deciding whether that visitor is allowed to do what they are asking is the plugin's job, not Joomla's.

In Helix Ultimate before 2.2.7, several of those actions did their work before checking a session token or a user permission. Here is what that exposed, roughly in order of how much it should worry you.

An unauthenticated write to your menus, leading to cross-site scripting

This is the one to care about. The framework's main AJAX handler took a `task` value, split it into a class and method name, and called the matching code. Some of those methods wrote to the database with no token and no permission check in front of them, including the code that saves mega menu settings onto a menu item. So an anonymous request could store attacker-controlled content in a menu item's parameters.

On its own that is bad enough. It gets worse because the menu and mega menu output was not escaped before being rendered, which is the cross-site scripting the changelog refers to. Stored content plus unescaped output is the textbook recipe for a stored XSS: a script the attacker plants once, that then runs in the browser of everyone who views the affected page. And a Joomla menu renders on more or less every page, including the administrator. Script that fires in a logged-in Super User's browser is the classic road to a freshly created admin account and a backdoor. That is why an "unauthenticated write to a menu setting" is not the minor-sounding issue it first appears.

An in-folder arbitrary file delete

The media manager's delete action was gated by a CSRF token but had no permission check and no proper path validation. The path you asked it to delete was joined onto the site root and passed more or less straight to the delete. Joomla's input filtering blocks the obvious `../../` climb out of the web root, but a single traversal step inside a valid path still slipped through, so a request could delete files anywhere inside your Joomla folder: `configuration.php`, an `.htaccess`, extension files, and so on. Because the only gate was a token rather than a real permission check, this was reachable by any logged-in user who could obtain a token, or by tricking a logged-in administrator into loading a malicious page (a cross-site request forgery). 2.2.7 adds the missing permission checks and confines the path properly.

An open redirect

The framework read a `helixreturn` value from the URL, base64-decoded it, and redirected the browser to it with no validation. That is a classic open redirect: an attacker crafts a link that looks like it points at your trusted domain but bounces the visitor off to a phishing page. 2.2.7 validates the decoded target and only redirects to internal URLs.

An unprotected template export and loose uploads

Two smaller items round it out. The template settings export ran without checking that the requester had permission to manage templates, which leaks configuration to anyone who asks. And the media upload validation was loose enough that the release tightened it to image types only, explicitly blocking SVG and ICO in the media manager (both can carry active content). The changelog also notes it stopped media uploads from accidentally triggering a template style import, and stripped internal server paths out of upload error messages so they stop leaking your directory structure.

How 2.2.7 closes it

The shape of the fix is reassuring, because it is consistent rather than a series of one-off patches. The old code trusted the request. The new code verifies it, the same way, across every action. Here is the release mapped to what each piece addresses.

Hardening in 2.2.7	What it fixes
A shared guard that runs a CSRF token check and a permission check in front of every AJAX action	Stops anonymous and unauthorised requests reaching the menu write, media, export and other handlers (the CWE-862 missing-authorisation class)
Menu and mega menu settings restricted to a known set of valid attributes before they are saved	Stops arbitrary attacker-controlled data being written into menu parameters
Output escaping added to media embeds, galleries, Mega Menu, Layout Builder and font options	Fixes the stored and reflected cross-site scripting (CWE-79)
Redirect targets validated and restricted to internal URLs only	Kills the open redirect through `helixreturn`
Corrected path validation in media, layout and blog file operations, confining them to their intended folders	Kills the in-folder file delete and related traversal
Permission checks added to blog image removal and template settings export	Stops unauthorised deletion and configuration disclosure
Upload validation restricted to image types, with SVG and ICO blocked in the media manager	Removes upload vectors that can carry active content
Frontend article saving restricted to valid Helix Ultimate attributes; direct POST access replaced with Joomla's input filtering; internal server paths stripped from upload error responses	Closes mass-assignment, unfiltered input and information-disclosure gaps

Is this a zero-day?

No, and it is worth being precise, because the word gets thrown around. A zero-day is a flaw that is being exploited before a fix exists. That is not what happened here.

JoomShaper's own team wrote and shipped the fix. The security changes went in as a single pull request that was merged and tagged as the 2.2.7 release within about two minutes of each other on 7 July 2026. The code and the patch became public at the same instant, there is no CVE, no security advisory was published, and nobody has reported exploitation in the wild. We confirmed the details by reading the public code difference between the old and new versions, not by finding a compromised site.

What this is, is an n-day risk: the moment a security fix ships, the patched code becomes a map. Anyone can line 2.2.7 up against the old version and work out exactly what each change is defending against, which is precisely how a stored XSS or an unauthenticated write gets turned into a working exploit. That is the clock every unpatched site is now racing.

The recurring pattern behind this

We keep writing about the same root cause because it keeps happening: an AJAX endpoint that Joomla will run for anyone, where the plugin checks a token, or nothing at all, but never checks who is actually calling it. A CSRF token confirms the request came from your own page; it does not confirm the person is allowed to make it. Authorisation is a separate step, and it is the one that keeps getting left out.

The same shape turned up in Novarain, in the Astroid framework, in SP Page Builder, in PageBuilder CK, and in Helix3 the week before this one. Helix Ultimate 2.2.7 is the same lesson again, and the fix, a single shared guard that enforces both a token and a permission on every action, is the right one. If you develop Joomla extensions, that shared-guard pattern is the thing worth copying.

What you should do right now

1. **Find every Helix Ultimate install you run.** If you use mySites.guru, search your extension inventory for Helix Ultimate and you have the list in seconds. If you do not, you will need to check each site's installed extensions by hand.
2. **Update every one of them to Helix Ultimate 2.2.7.** The update is live on JoomShaper's update server and shows in the normal Joomla updater. The framework installs as more than one piece, so update everything Helix Ultimate the updater offers, not just one of them. Unpublishing the plugin is not enough on its own, because the files stay on the server and the AJAX endpoint can still be reached directly.
3. **Do not confuse Helix Ultimate with Helix3.** They are separate products with separate updates. This one is Helix Ultimate 2.2.7.
4. **Check exposed sites for tampering.** Because the flaws allowed menu writes and file deletes, a site left unpatched could already have been touched. Check your menus and mega menu settings for entries you did not add, confirm protective files like `.htaccess` are still where they should be, and look at your Joomla Users list for Super User accounts you do not recognise. Our guides on finding hacked files and backdoors and fixing a hacked Joomla site walk through this.

If you would rather not do any of that by hand across a portfolio of client sites, that is exactly the job mySites.guru exists for. One inventory, every site, every framework version, one click to update. Run a free audit and see what is actually installed across your sites.

Further Reading

- Download Helix Ultimate - JoomShaper's download page, where the 2.2.7 release and its full changelog live.
- Using the Joomla com_ajax interface - how the unauthenticated endpoint works.
- CWE-862: Missing Authorization - the weakness class behind the missing permission checks.

- CWE-79: Cross-site Scripting - the weakness class behind the menu and Layout Builder XSS.
- Joomla Vulnerable Extensions List - the community-run list of known Joomla extension issues.

Frequently Asked Questions

What does Helix Ultimate 2.2.7 fix?

A batch of security holes in the Helix Ultimate template framework, most of them in its com_ajax handler. Before 2.2.7 several AJAX actions ran with no CSRF token check and no permission check, so an anonymous visitor could write to your site's menu settings (which, combined with unescaped output, opens the door to stored cross-site scripting). It also fixes a path-validation flaw that allowed file deletions inside your Joomla folder, an open redirect through the helixreturn parameter, an unprotected template settings export, and it tightens media upload validation. The full changelog is on JoomShaper's download page, tagged CWE-862 (missing authorisation) and CWE-79 (XSS).

Is this a zero-day?

No. A zero-day is a flaw being exploited before any fix exists. Here the fix and the code became public at the same moment: JoomShaper merged the security pull request and tagged the 2.2.7 release within two minutes of each other on 7 July 2026. There is no evidence of exploitation in the wild, no CVE has been assigned, and no security advisory was published. That said, now the patched code is public anyone can compare it against the old code to understand the bugs, so unpatched sites are a realistic target from here.

Is Helix Ultimate the same as Helix3?

No, and it matters because they patched security holes days apart. Helix Ultimate is JoomShaper's newer template framework, installed as the helixultimate system plugin plus the shaper_helixultimate template. Helix3 is the older, separate framework, which had its own unauthenticated file write and delete fixed in Helix3 3.1.1 on 29 June 2026. This post is about Helix Ultimate 2.2.7. If you run sites on both, each needs its own update.

Which versions of Helix Ultimate are affected?

Every version below 2.2.7. The last public release before it was 2.2.4 (22 January 2026), so if you are on 2.2.4 or anything older, you are exposed. Across the Joomla sites we monitor, most Helix Ultimate installs are a long way behind, still on the 2.1 or even 1.1 line, so the real-world exposure is wider than just recent installs.

Do I need to check my site for tampering, or is updating enough?

Updating stops the next attempt but does not undo anything that already happened. Because the flaws allowed an anonymous visitor to write to your menus and delete files, an unpatched site could already have been touched. After you update, check your menu and

mega menu settings for entries you did not add, confirm protective files like .htaccess are still in place, and look at your Joomla Users list for any Super User accounts you do not recognise, since a stored-script attack aims straight at your admin login.

How do I find every Helix Ultimate install across the sites I manage?

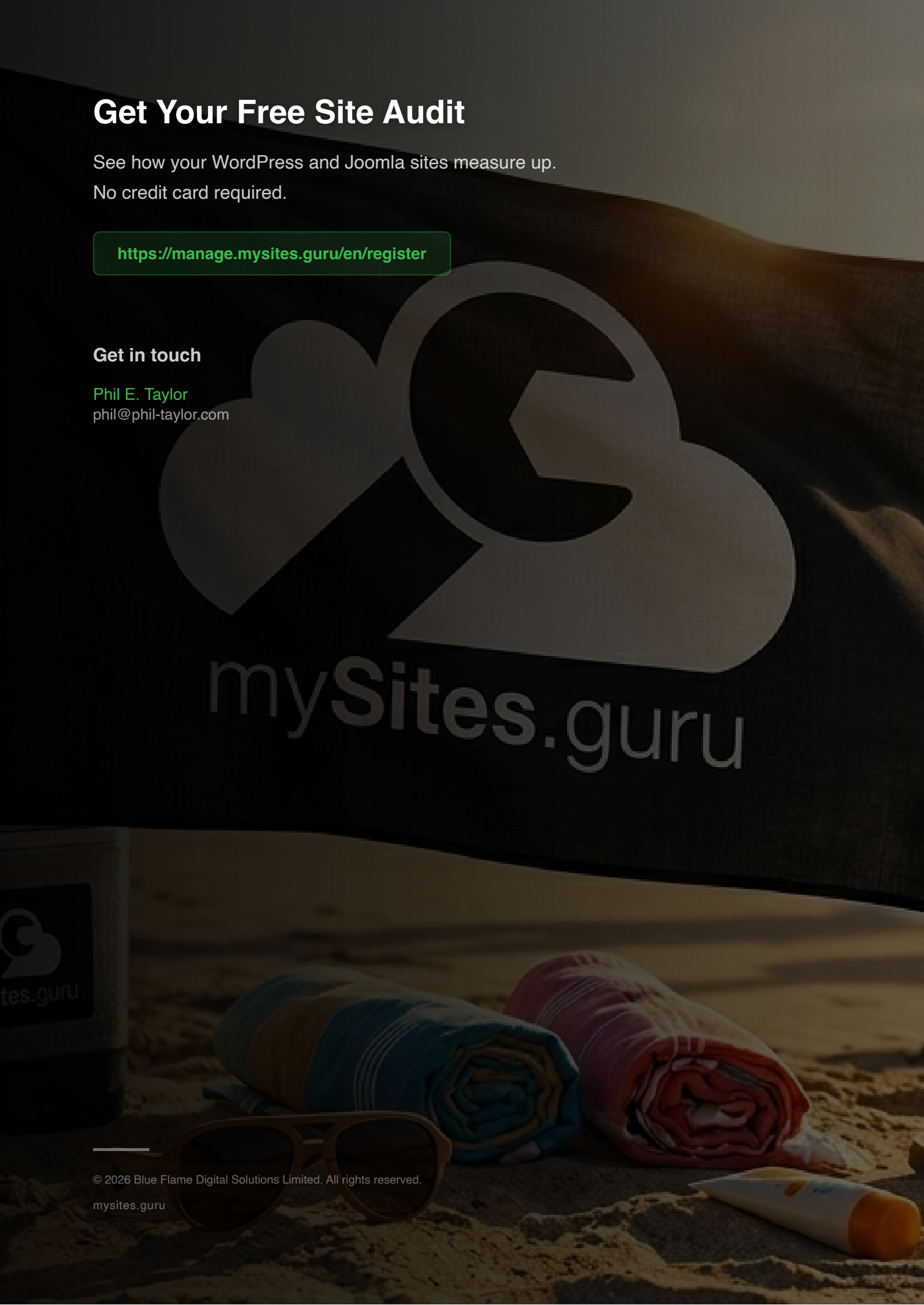
mySites.guru keeps a live inventory of every extension, template and framework on every Joomla and WordPress site in your account. Search for Helix Ultimate once and you get every affected site, the installed version, and a one-click path to push the 2.2.7 update, without logging into each site by hand. Start with a free audit at /free-audit/.

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