mySites.guru

Membership Pro 4.6.2: A Quiet Fix for Anonymous File Uploads

JoomDonation shipped Membership Pro 4.6.2 with the same anonymous file upload fix we reported in Events Booking. No CVE, no changelog. What to do about it.

Phil E. Taylor | 21 July 2026

Active Joomla Extension security alerts: Thirteen vulnerabilities found this month • JCE • Quix • SP Page Builder • jDownloads • EDocman

Membership Pro is one of the most widely used membership and subscription components for Joomla. It runs paid memberships, recurring subscriptions and gated content, which means the people signing up are handing over their details, and sometimes their money, to a form on your site. On 21 July 2026 its developer, JoomDonation, released **Membership Pro 4.6.2** with what the customer email calls "security improvements for file upload handling."

Read that phrasing next to what we published the day before. We had just reported an unauthenticated file upload flaw in Events Booking, the event registration component from the **same developer**, built on the **same controller framework**, with the **same File custom field upload feature**. Membership Pro 4.6.2 is that fix, applied to the sister product.

WHAT CHANGED

Before 4.6.2, having Membership Pro installed meant an unauthenticated visitor could upload files to your web server, whether or not your site used the feature that upload belongs to.

The vendor's own release notes describe them as "unauthenticated upload files" and ship a tool to delete the ones already left behind.

If you run Membership Pro on any Joomla site, update to **4.6.2** now and run the cleanup tool it ships. Everything at or below 4.6.1 is affected.

A note on what we know. We found and reported the anonymous upload flaw in Events Booking, which carries three CVEs. We have not pulled the Membership Pro source apart line by line the way we did Events Booking, and we do not need

to. This account is built on JoomDonation's own release email for 4.6.2 and on our full audit of the identical flaw in its sibling component. Where we are inferring rather than confirming, we say so.

TL;DR

- **Membership Pro 4.6.2 fixes an unauthenticated file upload endpoint.** Subscribers upload files through it when a site uses File custom fields, and before 4.6.2 it was reachable by anonymous visitors even on sites that had never created a File field
- **It is the same flaw, and the same fix, as** Events Booking, from the same developer and the same codebase, which we reported and which carries three CVEs
- **There is only one plausible reason 4.6.2 exists.** Having had the bug demonstrated in one product, JoomDonation closed it in the sister product built on the same framework, one day after emailing Events Booking customers
- **The release admits the exposure in its own words.** 4.6.2 "automatically disables the upload endpoint when your site does not use any File custom fields, reducing unnecessary exposure" and ships a cleanup tool to "remove any unauthenticated upload files that may have been left behind"
- **No CVE, no advisory, no changelog entry.** Customers were emailed that this is "a security improvement rather than a vulnerability" and "not a critical security issue"
- **An anonymous upload path is not a footnote.** It is free, unattributable storage on your domain, and attackers go looking for exactly that
- **Update to 4.6.2, then run the cleanup tool.** The tool deletes upload files with no matching subscription record. There is a scheduled task version to keep doing it
- **Almost nobody is on the fix.** Across the Membership Pro installs we can see on our customers' sites, fewer than one in a hundred were on 4.6.2 when we looked, and the single most common version was 4.6.1, the exact release it replaced

Why does Membership Pro 4.6.2 exist?

There is only one plausible reason, and it is us. We did not report a flaw in Membership Pro. We reported one in Events Booking, and Membership Pro 4.6.2 is what happened next.

The case is circumstantial but it is not thin. Events Booking and Membership Pro are both JoomDonation products. Both run on the same in-house controller framework, the one whose front-end dispatcher performs no CSRF check and no permission check by default and leaves each method to guard itself. Both offer File custom fields, the feature that lets a form collect an uploaded file during sign-up. And both, before their respective fixes, exposed that upload to anonymous visitors on every install.

When we disclosed the Events Booking upload, the developer re-reviewed that codebase and shipped a series of changes to the endpoint. The tell is the timing and the shape. JoomDonation emailed Events Booking customers on 20 July. Membership Pro 4.6.2 was released on 21 July with an upload fix described in almost the same language, down to the phrase “unauthenticated upload files” and a cleanup tool that does the same job as the orphan file cleanup tool shipped for Events Booking. A developer does not audit and re-engineer a specific upload endpoint across two products in a week for no reason. The reason was the report on the first one.

We think that is the correct thing to have done, and we will say so plainly: finding a class of bug in one product and going to close it in your others is exactly the response you want from a vendor. Our objection is to how the release was announced, and to what the people who need to act were told about it.

What the release email admits

The customer email for 4.6.2 is the best evidence for what the flaw was, because it describes the fix while trying not to describe a vulnerability. Two sentences do the work.

First: the upload endpoint “is now automatically disabled when your site does not use any File custom fields, reducing unnecessary exposure.” The word doing the lifting there is “now.” If disabling the endpoint on sites without File fields reduces exposure, then that exposure existed before, on every install that had Membership Pro present and had never touched the upload feature. That is the same defect the Joomla CNA recorded for Events Booking: an upload that was live by default, whether the site asked for it or not.

Second: the email recommends running “the new cleanup tool included in Membership Pro 4.6.2 to remove any unauthenticated upload files that may have been left behind before the update.” The vendor’s own words are “unauthenticated upload files.” You do not ship a tool to delete a category of file unless that category exists and you expect to find it in the wild.

Set against those two admissions is the framing wrapped around them. The email calls the change “security improvements” rather than a vulnerability, states in bold that it is “not a remote code execution vulnerability,” and closes that “while this is not considered a critical security issue, we recommend updating.” At the time of writing there was no changelog entry for 4.6.2 on JoomDonation’s public changelog at all, no CVE, and no security advisory. The only public account of this release is an email that tells you it is nothing to worry about.

That combination is the reason to worry a little. A fix for an anonymous write path into your web server, shipped with no CVE, no advisory, no changelog line, and a note telling customers it is not critical, is the outcome least likely to get anybody to install it.

Why an anonymous file upload is such a problem

Code execution is the loudest thing an unauthenticated upload can buy an attacker, and treating it as the only thing that counts is how this kind of finding gets waved through. On a default configuration, this is not code execution, and we are not going to pretend it is. It is a stranger with write access to your file system, which is quite bad enough.

Anonymous, unattributable file storage on somebody else's infrastructure is a commodity, and people go looking for it. An open upload endpoint on a legitimate business domain is close to ideal for that: it costs nothing, it is not registered to anyone, the bandwidth is billed to a stranger, and the content inherits the reputation of a real site with a real TLS certificate that no filter has any reason to block.

What ends up in those folders is not theoretical. Pirated media and warez, because someone else is paying for the disk and the transfer. Phishing kits and fake login pages, which work far better when the URL is a genuine company domain than when it is a throwaway host. Malware and droppers staged for a different campaign entirely, so the attack on somebody else runs through your server. And illegal imagery, including material involving children, parked somewhere the people trading it will not be traced.

The part that matters for you is that all of it arrives with your name on it. You signed the hosting contract. The IP address, the domain and the billing details are yours. When the abuse report is written it is addressed to you, and hosts generally suspend first and investigate afterwards, which means the first thing you know about it may be a dead site and a support ticket. Beyond that sit domain and IP blocklisting, a payment processor taking an interest, and for the worst categories of content a set of legal obligations considerably more serious than a hosting suspension.

We have watched this happen. The Balbooa Forms flaw we disclosed this month did not come to us from a code audit. It came from a Hetzner abuse report sent to one of our customers, who brought us the raw access log. That is what an anonymous upload endpoint looks like from the owner's side: a message from your host telling you your server has been doing something you knew nothing about.

The quiet part is that you will probably not notice on your own. Nothing errors. No page breaks. Files accumulate in a directory nobody has any reason to open, attached to no subscription, and the site carries on serving memberships exactly as it did before.

Is this remote code execution?

Not on a default configuration, and the vendor is right about that much. A file upload constrained to image and document types cannot drop a web shell, so “not a remote code execution vulnerability” is a fair description of the shipped defaults. We said the same thing throughout our Events Booking write-up.

The problem is the absolute claim underneath it. The list of permitted file types is an administrator-editable setting. On a site whose owner has widened it to accept an executable type, which is unusual but not unheard of where a form needs to accept unusual attachments, an anonymous upload becomes straightforward unauthenticated remote code execution. “Attackers could not upload executable files” is true of the defaults, not of every install, and a message sent to every customer is making a promise about every install.

This is the same shape as the file upload flaws we found in PageBuilder CK and RSFiles!, which were clean unauthenticated RCE, and it sits one configuration change away from joining them. How serious it is for you depends on your allowed file types and on how long your site ran an affected version with a public sign-up form. A new membership site nobody has found yet is probably fine. A site that has been in Google for years has been reachable by every scanner on the internet for as long as this code has existed.

What Membership Pro 4.6.2 actually changes

From the vendor’s own description, 4.6.2 does three things to the upload path, and each maps onto a specific weakness in the versions before it.

- **The endpoint is disabled when no File custom fields exist.** This is the headline fix. The upload is no longer live on installs that were not using it, which is the “unnecessary exposure” the email refers to. If your site has no File fields, 4.6.2 takes the endpoint off the board entirely.
- **Validation and abuse protection are added when File fields are in use.** Sites that do collect uploads keep the feature, now with additional checks on what gets accepted. The email does not enumerate them, and without a changelog we are

not going to guess at the specifics, but this mirrors the rate limiting, per-field permission checks and content validation JoomDonation added to Events Booking.

- **A cleanup tool removes files already left behind.** The new tool deletes upload files with no matching subscription record, and a scheduled task can run it on a timer.

There is no version below 4.6.2 that is safe here. The fix is the update, and unlike a SQL injection there is no malicious payload for a web application firewall to recognise. The attack is an ordinary, well-formed upload request that the site is designed to answer. The only thing wrong with it is who sent it, and your firewall has no way to know that. Updating is the whole of the defence.

Run the cleanup tool after you update

Updating closes the door. It does not empty the room behind it.

DO THIS AFTER YOU UPDATE

Membership Pro 4.6.2 ships a tool that finds and deletes every file in the upload folder with no matching subscription record.

Run it even if you are certain you were never a target. It is the only way to see what that endpoint accepted while it was open, and there is a scheduled task version so it keeps checking.

The vendor documents both the cleanup tool and the scheduled task, the latter with a retention window that defaults to 72 hours. The documentation defines an orphan file as one “upload by users but not associated to any subscription records”, which is the vendor describing, in a help page written before any of this, a file that arrived on your server from somebody who never completed a subscription. If the tool finds nothing, that is good news you can only get by looking. If it finds files you do not recognise attached to no subscription, treat the site as having hosted content you did not put

there, and work through our guide to finding hacked files and backdoors in Joomla before you assume it was harmless.

Almost nobody is on the fixed version

Here is the part of this story that worries us more than the flaw does, and it has nothing to do with how clever the bug is.

We can see Membership Pro installed on just over **440 Joomla sites** across our customers' accounts. When we checked which versions those sites were running the day 4.6.2 shipped, we did not find a well-updated majority with a few stragglers behind it. We found this:

Version line	Share of installs
4.6.2 (the fix)	under 1%
4.6.0 or 4.6.1 (one or two releases behind)	~44%
4.x below 4.6	~32%
3.x or older	~23%

Read the top two rows together. Fewer than one install in a hundred had taken the fix, and the single most common version across every site was **4.6.1, the exact release 4.6.2 replaces**. Nearly a quarter of installs were an entire major version or more behind, some of them still on 2.x and 1.6 builds that are years old.

This is the uncomfortable truth behind every quiet security release. A fix now exists that will reach approximately nobody, because the sites running this extension were already far behind before the update shipped, and this one arrived with nothing but an email telling customers it was not critical. If you manage Joomla sites and have not looked at your extension versions recently, that table is probably a description of your own portfolio. I have never met an administrator who decided 4.4.1 was good enough. What I have met is a lot of people for whom updating an extension means logging

into each site's admin one at a time, a job that grows with every client, so it waits until something breaks.

How do I find every Membership Pro site I manage?

The awkward question after any extension security release is which of your sites actually run the thing. Up to about ten sites you can log into each Joomla admin and read the installed extensions list. Past that you need a single view, which is precisely why those version numbers get so old: the work of checking scales with the number of sites, so it stops happening.

mySites.guru keeps a live inventory of every extension, template and framework on every Joomla and WordPress site in your account. Search for Membership Pro once and get back every connected site running it, the version each one is on, and whether an update is available. That is the same query we ran to produce the version table above, and you can run it against your own sites in about ten seconds.

View every Membership Pro install across your sites

Open your Extension Inventory

Search for Membership Pro across every connected Joomla site and filter for anything below 4.6.2. Not a subscriber? Sign up free and connect your sites.

Once you know which sites need it, the mass updater handles the rollout. When a fix ships we add the affected range to our vulnerability database, so every connected site still on a version below 4.6.2 is flagged automatically. You can also enable auto-updates for any Joomla extension so the next fix like this one reaches your sites without you lifting a finger. You should not have to hear about a Joomla security release through a mailing list you might not be on, then audit a portfolio of client sites by hand to find out whether it is your problem.

What to do right now

- Update every Joomla site running Membership Pro to **4.6.2** or later, one at a time or in bulk from one dashboard
- **Take a backup first.** Before any extension update on a production site, trigger a snapshot or a full backup so you have a clean starting point
- **Run the cleanup tool** after updating, to delete any unauthenticated upload files left behind, and consider the scheduled task version
- If you are on a build several versions back, expect a real upgrade rather than a one-click patch, and test it somewhere other than production
- Do not rely on a firewall for this one. There is no payload to filter, so there is nothing for it to block
- If you manage multiple sites, let mySites.guru show you which ones are still exposed rather than checking by hand
- If the cleanup tool finds files you cannot account for, treat the site as potentially compromised and follow our guide to fixing a hacked Joomla or WordPress site

Stay ahead of the next one

There will be another one, because Joomla runs on thousands of third-party extensions and the ones that accept anonymous input keep producing bugs like this. This is the second JoomDonation upload endpoint to be hardened in a week, and it will not be the last extension to close a hole like this with no CVE and a reassuring email. The hard part was never the update itself. It is knowing a fix exists, knowing which of your sites are affected, and getting to them before someone else does.

That is the job mySites.guru does. It keeps a live inventory of every extension on every Joomla and WordPress site in your account, flags the ones with a known vulnerability, and lets you push the update to all of them from one screen. When something like this is disclosed you see exactly which sites are exposed in seconds, without opening a single admin panel.

Get free email alerts when a Joomla vulnerability breaks

We email a plain-English alert the moment a serious flaw like this one is disclosed, with the affected versions and what to do. No charge, unsubscribe any time.

Subscribe to security alerts

Want the alerts and the tooling to act on them? Start with a free audit on one site and see your full extension inventory, or sign up for mySites.guru to get vulnerability alerts and one-click updates across every site you manage.

Disclosure and severity

What we are and are not claiming

We did not discover or report a vulnerability in Membership Pro, and no CVE has been assigned to it. We reported the identical anonymous upload flaw in Events Booking, which carries CVE-2026-60024 and CVE-2026-60025. This post reads across from that audit and from JoomDonation's own 4.6.2 release email. Our assessment of the Membership Pro upload is the same as our assessment of the Events Booking one: **Medium** on a default configuration, with a **High** ceiling on any site whose allowed file types have been widened to an executable type, where it becomes unauthenticated remote code execution.

Field	Detail
Component	Membership Pro for Joomla (`com_osmembership`)
Vendor	JoomDonation / Ossolution (joomdonation.com)
Type	Unauthenticated file upload (CWE-434)
CVE	None assigned. No advisory, no changelog entry at time of writing
Impact	Anonymous file writes to the web server, on installs that were not using the upload feature
Affected versions	4.6.1 and earlier
Fixed in	4.6.2, released 21 July 2026

Field	Detail
Related disclosure	Events Booking, same developer, same flaw class, reported by Phil Taylor of mySites.guru

Further Reading

- Our Events Booking disclosure - the anonymous upload flaw we reported in the sibling component, with the full technical detail and the three CVEs behind this fix.
- This was one of a month of Joomla extension vulnerabilities we found and disclosed - the wider run this fits into.
- Why AJAX endpoints are a CMS security blind spot - the opt-in security pattern in JoomDonation's controller framework that produces findings like this one.
- CWE-434: Unrestricted Upload of File with Dangerous Type - the canonical reference for this weakness class.
- Membership Pro product page - where 4.6.2 is available to download.

Frequently Asked Questions

What did Membership Pro 4.6.2 fix?

Membership Pro 4.6.2, released on 21 July 2026, hardens the file upload endpoint that subscribers use when a site has File custom fields. In earlier versions that endpoint accepted uploads from unauthenticated visitors, and it stayed reachable even on sites that were not using any File custom fields. 4.6.2 automatically disables the endpoint when no File fields exist, adds validation and abuse protection when they do, and ships a cleanup tool to delete the unauthenticated upload files earlier versions had already accepted. It is the same class of flaw, and the same fix, that we reported to the same developer in Events Booking.

Is there a CVE for the Membership Pro upload issue?

No CVE has been assigned, there is no security advisory, and at the time of writing there was not even a changelog entry for 4.6.2 on JoomDonation's public changelog. Customers received an email describing the change as a security improvement rather than a vulnerability. That absence of a public record is exactly why a tool that tracks your extension versions matters more than a mailing list you might not be on.

Am I affected if my site does not use File custom fields?

On any Membership Pro below 4.6.2, yes. The whole point of the 4.6.2 change is that the upload endpoint used to be live regardless of whether you had created any File custom fields. The vendor's own email describes the new behaviour as automatically disabling the endpoint when your site does not use File fields, to reduce unnecessary exposure, which is an admission that the exposure was there before. Update to 4.6.2 and the endpoint switches off on sites that do not need it.

Which Membership Pro version do I need?

Update to Membership Pro 4.6.2 or later. Treat every version at or below 4.6.1 as affected. Because Membership Pro versions its component on its own numbering, this is not a Joomla 3 versus Joomla 4 question: 4.6.2 is simply the current release, and anything older carries the un-hardened upload endpoint.

Is this remote code execution?

Not on a default configuration, and the vendor is right to say so. A file upload constrained to image and document types is not a web shell. What it is, is an anonymous stranger with write access to your server, on a legitimate business domain, whose files the site can then

serve back to anyone. That is enough to host malware, phishing pages, pirated media or worse, all under your hosting contract and your name. If an administrator has widened the allowed file types to include an executable type, it becomes straightforward unauthenticated remote code execution.

Should I run the cleanup tool after updating?

Yes. Membership Pro 4.6.2 ships a tool that finds and deletes upload files left behind with no matching subscription record, and there is a scheduled task version to keep doing it. Run it even if you are certain you were never a target. It is the only way to see what that endpoint accepted while it was open, and the vendor recommending it is itself a signal that unauthenticated files do end up in that folder.

How do I find every Membership Pro site I manage?

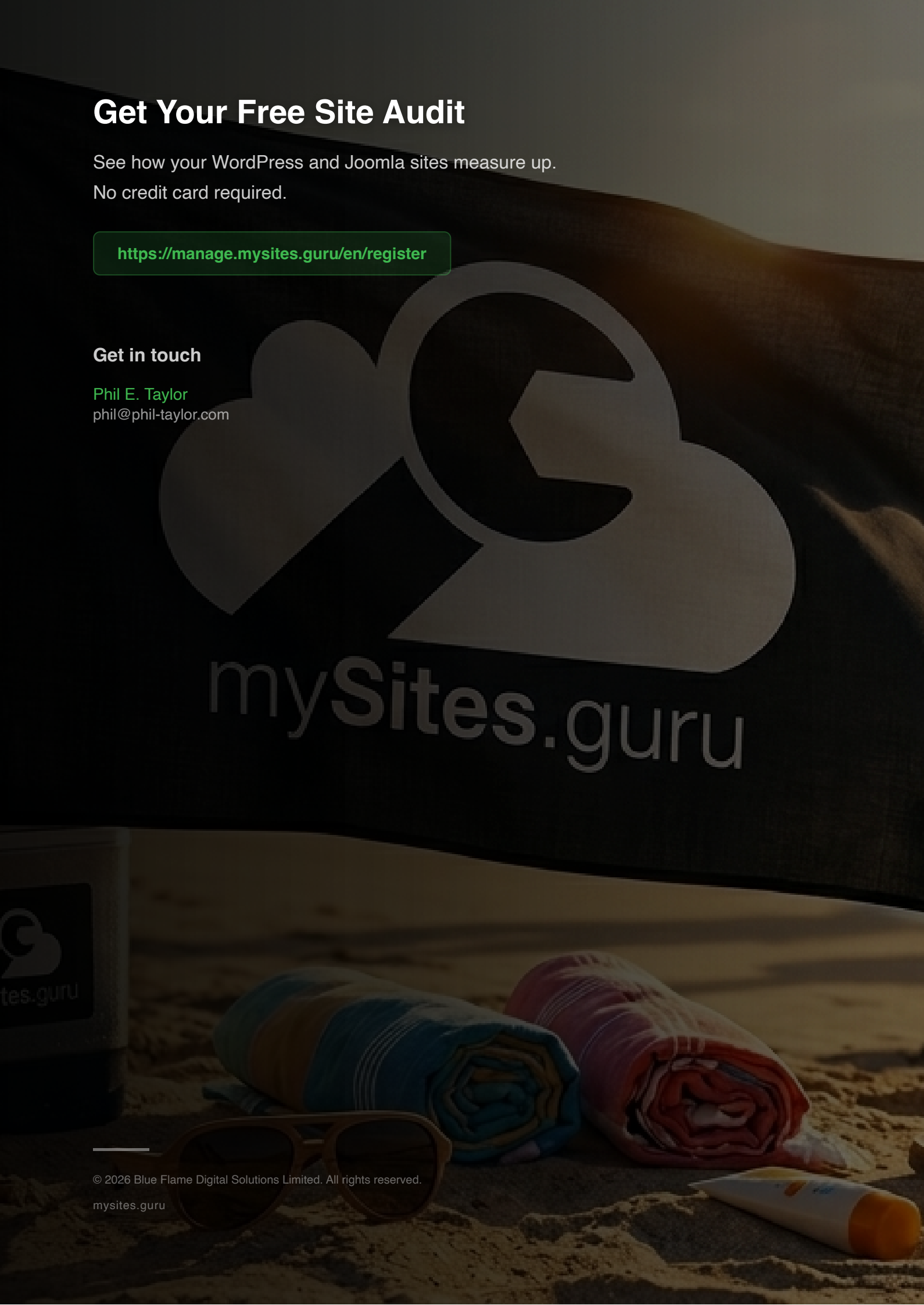
mySites.guru keeps a live inventory of every extension and version on every connected Joomla and WordPress site. Search for Membership Pro once and get back every site running it, the version each is on, and whether an update is available. Every connected site still on a version below 4.6.2 is flagged automatically against our vulnerability database, so you do not have to audit a portfolio of client sites by hand.

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