mySites.guru

JCE Free/Pro 2.9.99.5 Patches an Unauthenticated File Upload in Joomla's Most-Installed Editor

JCE Free and JCE Pro 2.9.99.5 patch an unauthenticated editor profile upload that could be used to upload arbitrary files to the server. Update every Joomla site running JCE now.

Phil E. Taylor | 3 June 2026

JCE (Joomla Content Editor) ships on more Joomla sites than any other editor extension. It sits in the top two of our live extension ranking, neck and neck with Akeeba Backup. If you look after a stack of Joomla sites, the odds that nearly all of them have JCE installed are very high.

On 3 June 2026, the JCE developer released JCE Pro 2.9.99.5 and the matching JCE Free 2.9.99.5. The changelog carries one security line, and it is the kind you act on the same day: **insufficient access controls permitted unauthenticated users to upload editor profiles**, which the developer states could be exploited to upload arbitrary files to the server.

This is the second JCE security release in a week. The 2.9.99.4 release on 28 May patched two bugs that both required a logged-in session. This one does not. That single difference, authenticated to unauthenticated, is what moves it from “patch this week” to “patch now”.

This post covers what was patched, how the flaw differs from last week’s, what an attacker could do with it, and how to find and update every vulnerable JCE install across the Joomla sites you manage with mySites.guru instead of one administrator panel at a time.

> **The short version**
>
> An unauthenticated visitor could upload an editor profile, and a profile controls what filesystem and upload actions JCE permits. The developer says this could be used to upload arbitrary files to the server. Every Joomla site running JCE is in scope, not just ones with public registration. Update to 2.9.99.5 today.

TL;DR

- **JCE Pro 2.9.99.5** and **JCE Free 2.9.99.5** released 3 June 2026
- Fixes insufficient access controls that let **unauthenticated** users upload editor profiles, which the developer says could be exploited to upload arbitrary files to

the server

- Affects **all versions of JCE Free and JCE Pro before 2.9.99.5**
- This is a **separate, more serious flaw** than the authenticated-only bugs patched in 2.9.99.4 a week earlier, not a reopening of them
- **No login is required**, so every Joomla site with JCE is exposed regardless of registration settings
- No CVE number assigned at time of writing. That does not lower the severity
- Runs natively on Joomla 3, 4, 5, and 6 without the Backwards Compatibility plugin
- Reported by Uwe Flottemesch of fc-hosting.de, with assistance from David Jardin, lead of the Joomla Security Strike Team
- Update via the Joomla Update Manager or the JCE downloads area
- If you manage multiple sites, mySites.guru's mass updater pushes the update to every affected site in one batch

What was patched in JCE 2.9.99.5?

The security line in the 2.9.99.5 changelog reads, verbatim:

> *"Insufficient access controls permitted unauthenticated users to upload editor profiles."*

The release announcement adds that the flaw "could be exploited to upload arbitrary files to the server." To see why those two sentences belong together, you need a quick refresher on what an Editor Profile actually is.

A quick tour of JCE Editor Profiles

JCE's defining feature is its Editor Profiles system. Rather than handing every logged-in user the same editor, JCE lets an administrator define different profiles for different user groups. A registered user might get a stripped-down toolbar with no file uploads.

A content editor might get image and file managers scoped to one media directory. A super user gets the full editor with broad file operations.

Each profile defines:

- Which toolbar buttons are visible
- Which file types can be uploaded
- Which directories the editor can browse and upload into
- Which advanced features (templates, code view, and so on) are exposed

A profile is, in effect, a set of filesystem permissions wearing an editor's clothes. Control the profile and you control what file operations JCE will carry out.

Why an unauthenticated profile upload is the dangerous part

The 2.9.99.5 flaw was an access control gap on the action that uploads (imports) an editor profile. Before the patch, that action did not properly check that the request came from an authorised, logged-in user. An unauthenticated request could reach it.

Put those two facts next to each other. If an anonymous actor can upload a profile, and a profile dictates which file types may be uploaded and into which directories, the attacker can define a profile permissive enough to allow the upload they want, then use it. That is the path the developer is pointing at with "upload arbitrary files to the server."

The vendor has not published a proof of concept, the exact controller and task, or a confirmed remote code execution chain, so treat the arbitrary-file-upload outcome as the realistic risk the patch closes rather than a demonstrated exploit. The mechanism does not need a working public exploit to deserve same-day patching. Unauthenticated plus file upload is a combination you close immediately and ask questions later.

How 2.9.99.5 differs from last week's 2.9.99.4

It is reasonable to assume a second JCE release in a week means the first fix was incomplete. That is not what happened here. The two releases address different

vulnerabilities in the same area of code.

	JCE 2.9.99.4 (28 May)	JCE 2.9.99.5 (3 June)
Authentication	Required a logged-in session	**None required**
Affected area	File browser	Editor profile upload
What it fixed	Editor Profile access check plus a directory traversal in filesystem search	Access control on the profile upload action
Severity	Moderate, bounded by profile permissions	High, unauthenticated path to file upload

The 2.9.99.4 release tightened the file browser: it stopped an authenticated user from invoking actions through an Editor Profile they were not assigned to, and it closed a directory traversal in the filesystem search. Both required an account. The 2.9.99.5 release closes a different door, the one that lets a profile be uploaded in the first place, and that door was open to anyone.

The two clearly come from the same coordinated review of JCE's profile and filesystem handling, which is a good thing. A thorough audit of one component tends to surface a cluster of related issues, and JCE's developer has shipped fixes for the lot within days of each report.

A note on JCE's history with file uploads

There is a reason an unauthenticated file upload in JCE specifically should make you move quickly, and it is not the 2026 bug. It is the 2012 one.

Back in 2012, an unauthenticated arbitrary file upload in JCE's ImageManager (tracked as CVE-2012-2902) became one of the most widely exploited Joomla vulnerabilities of its era. Automated bots scanned the internet for vulnerable JCE installs, uploaded an innocuous-looking image file, then renamed it to a `.php` extension to drop a web shell. Security vendors including Sucuri and Trustwave documented the campaign, and it

shipped as a ready-made module in Metasploit. Sites were still being compromised through it years after the patch existed, purely because so many were never updated.

The 2026 issue is a separate, newly patched flaw, and there is no evidence anyone is exploiting it as this post goes out. The history matters because of what it shows: when an unauthenticated JCE file-upload bug meets a long tail of installs nobody updated, you get mass, automated, opportunistic compromise. Nothing to panic about today. Plenty of reason not to be the site still running a vulnerable JCE in six months.

What an attacker could do, and what they could not

What the patch closes is an unauthenticated route to uploading an editor profile, and from there potentially to uploading files the site never intended to accept. On a site where that chain reaches an executable location, the worst case is the familiar one: a web shell, persistent backdoor access, and a site that needs a full clean rather than an update.

What the advisory does not claim is a turnkey, one-request remote code execution with a published exploit. There is no PoC in circulation and no CVE yet. What it does describe is an unauthenticated way in and a file-upload outcome the vendor has named outright. That is enough. You update to close it rather than wait to find out, on a site you manage, how far the chain actually reaches.

This puts 2.9.99.5 in a different and more urgent category than 2.9.99.4, and alongside genuinely unauthenticated Joomla issues like the Smart Slider 3 arbitrary file read and Novarain Framework's file inclusion, rather than the authenticated-only bugs from last week.

How to update JCE on a single Joomla site

For one site, the update is routine. Joomla's built-in extension update tooling will pick up 2.9.99.5 as soon as the JCE update server publishes it, which it has.

1. Log in to the Joomla administrator
2. Go to **System -> Update -> Extensions**
3. Click **Check for Updates**
4. Select the JCE row
5. Click **Update**

If the update does not appear, check that JCE's update site is enabled under **System -> Update -> Update Sites**. For JCE Pro, you also need a valid subscription key entered under **Components -> JCE Editor -> Options -> Subscription Key** for the Pro update channel to be reachable. JCE Free pulls updates from the Joomla extension feed and needs no key.

After updating, hard-refresh the editor in a logged-in session to flush cached JCE assets. The version under **Components -> JCE Editor** should read 2.9.99.5 once you reload.

How to find every Joomla site with a vulnerable JCE using mySites.guru

That is the easy case. The hard case is "I look after 40 client Joomla sites, and an unauthenticated file upload just got patched. Which of them are still vulnerable, right now?"

That is what mySites.guru is built for. Twice a day, a snapshot runs against every connected Joomla site and indexes every installed extension, including its exact version. You can answer the JCE 2.9.99.5 question in seconds instead of logging into 40 administrator panels in sequence.

Open the extension search in your dashboard and look up the **Editor - JCE** entry. You see every version of JCE across your portfolio, grouped by version number, with each site that runs it listed underneath. Anything on 2.9.99.4 or earlier needs the update. Sites already on 2.9.99.5, or which auto-updated overnight, are green.

You can also separate JCE Free from JCE Pro if you run a mixed estate. Both editions ship the same fix in 2.9.99.5 from the same update server, but Pro is gated by a subscription key, so it helps to know which sites sit in which group when you start chasing the stragglers.

mySites.guru subscribers: jump straight to the JCE inventory

Open JCE Extension Search

Lists every JCE install across your connected Joomla sites, grouped by version. Anything on 2.9.99.4 or earlier needs the 2.9.99.5 patch. Not a subscriber? Sign up free and connect your sites.

Push 2.9.99.5 across every affected site in one batch

Once you know which sites are vulnerable, you do not patch them one by one. The mySites.guru mass extension updater lets you select every site running an outdated JCE and trigger the update across all of them at once.

The mass update screen groups every JCE install by the version it can update to, with an "Apply to all" button per group and per-site controls when you want to be selective. Sites stuck on much older branches (2.6, 2.7, 2.8) get patched in the same sweep as ones already on the 2.9.99.x line. Behind the scenes, the platform calls each site's connector, pulls the 2.9.99.5 package from JCE's update server, installs it, and reports back with a pass or fail per site and a log entry against the site. Any site that is offline, firewalled, or running an outdated connector surfaces as a clear failure rather than a silent miss.

For agencies running scheduled automation, JCE updates can be enrolled in the same overnight extension auto-update flow as everything else. The Automatic Updates for Any Joomla Extension feature already covers JCE Free and JCE Pro through Joomla's native extension update API.

Sites with auto-updates enabled were patched overnight

This is exactly the scenario automatic extension updates exist for. The mySites.guru auto-updater pushes security releases like 2.9.99.5 to opted-in Joomla sites without anyone logging in. If your sites are enrolled, the patch has landed, the version is verified, and an audit entry is sitting in the activity log. If they are not, an unauthenticated file upload in your most-installed editor is a good reason to change that. Turn on automatic extension updates and the next time a popular extension ships a security fix, you wake up to "done" rather than "to do." Enable auto-updates from your dashboard or start a free trial if you do not have an account yet.

How quickly should you patch JCE 2.9.99.5?

Faster than you patched 2.9.99.4. Because this flaw is unauthenticated, the usual "only sites with registered users are at risk" reasoning does not apply. Any Joomla site with JCE installed is in scope.

Patch today on any site that is publicly reachable and runs JCE, which is almost all of them. There is no functional change in 2.9.99.5 that would justify holding back, and the update is free and config-free for both Free and Pro.

Patch within 24 to 48 hours at the outside, even for low-traffic brochure sites with no registration. "No registered users" was a mitigating factor for 2.9.99.4. It is not one here.

The risk calculus on an unauthenticated file upload is simple. Applying a clean security patch with no functional changes carries essentially no risk. Leaving it unpatched carries whatever a passing automated scanner decides to do with it, multiplied across every site you have not got to yet. JCE's own 2012 history is the cautionary tale.

Edge cases and gotchas

A few things to watch when rolling 2.9.99.5 across an estate.

Lapsed JCE Pro subscriptions

Both editions pull updates from JCE's own update server, not the Joomla Extensions Directory. The catch for Pro is the subscription key. If a Pro install's subscription has lapsed, 2.9.99.5 will not appear in that site's update list and the site sits silently on the vulnerable version. The fix is to renew, or to drop a temporary key into the site, pull the security release, then sort the renewal afterwards. A practical move is to scan your mySites.guru extension report 48 hours after release for any JCE Pro install still below 2.9.99.5. Those are almost certainly the lapsed subscriptions.

Sites still on JCE branches older than 2.9

A JCE 2.6.x or 2.7.x install on a long-tail Joomla 3 site is far more exposed than this single advisory implies. The 2.9.99.5 fix is for the current branch. Older lines have not received it and carry years of unpatched issues on top. The right answer is to bring both Joomla and JCE up to date together. mySites.guru's migration tooling helps triage which sites need the most work. If a client genuinely refuses to modernise, at minimum disable JCE on that site and fall back to TinyMCE or CodeMirror until it can be brought current.

Custom Editor Profiles with broad filesystem access

If you previously set up an Editor Profile with broad filesystem access (the whole `images/` tree, or worse), audit it after updating. The 2.9.99.5 patch closes the unauthenticated upload route, but least privilege still applies. A profile with broad file permissions remains a high-value target for whatever the next JCE issue turns out to be. Review every profile under **Components -> JCE Editor -> Editor Profiles** on each site and lock each one to the narrowest path that still lets its user group work.

Checking for signs of compromise

Unlike the authenticated 2.9.99.4 bugs, this one leaves a fingerprint you can hunt for, because the malicious request needs no session. A retrospective audit on a higher-risk site looks like this:

1. Pull the last 90 days of web server access logs and look for requests to JCE's profile and filesystem endpoints, including upload or import actions, that carry no

Joomla session cookie. Unauthenticated requests are the ones that matter here.

2. Audit your `images/`, `media/`, and any custom upload roots for files you did not put there, especially anything with a script extension or a recent timestamp that does not match a known change.
3. Look for unexpected files anywhere a profile upload could have reached, not only the obvious media directories.

If anything looks deliberate, treat the site as a suspected compromise: rotate Joomla secrets, invalidate active sessions, and run mySites.guru's suspect content scanner against the site to surface backdoors and modified files. For most sites the audit comes up empty, which is the point. Close the chapter deliberately rather than assuming nothing happened because nothing was reported.

JCE and the Joomla Backwards Compatibility plugin

The 2.9.99 branch is native to Joomla 5 and 6 and does not need the Backwards Compatibility plugin. If JCE is the only reason BC is enabled on a site, you can disable BC once 2.9.99.5 is in place, provided your other extensions are also BC-free. For an estate-wide audit of which sites still need BC, see our Joomla compat plugin is a crutch write-up.

Does this affect WordPress?

No. JCE is a Joomla-only editor extension. There is no WordPress build of JCE Pro or JCE Free, no shared codebase, and no equivalent advisory for WordPress. WordPress sites use the core block editor or TinyMCE, which have their own separate histories. If you run a mixed estate, the WordPress half is unaffected by this advisory. The Joomla half needs the update.

The shape of this bug, an access control missing on a request that should have required authorisation, is a recurring one across both platforms. We dug into it in AJAX Endpoints: The Biggest CMS Security Blind Spot, where endpoints that should

check who is calling them simply do not, from Smart Slider 3 to Joomla core's own `com_ajax` router.

Further Reading

- JCE Pro 2.9.99.5 release announcement - the developer's advisory and changelog
- JCE Free/Pro 2.9.99.4 Security Update - last week's authenticated-only release, for the full picture
- JCE downloads area - direct package downloads for JCE Pro subscribers
- JCE on the Joomla Extensions Directory - the JCE Free listing
- Top 50 Joomla Extensions - live ranking from the mySites.guru database, where JCE consistently ranks in the top two
- How to update Joomla, Joomla extensions, WordPress and WordPress plugins from mySites.guru - the mass updater workflow used for rollouts like this
- Automatic updates for any Joomla extension - enrol JCE in scheduled overnight updates so the next advisory patches itself
- AJAX Endpoints: The Biggest CMS Security Blind Spot - the recurring missing-authorisation pattern across Joomla and WordPress

---

For broader agency guidance on managing Joomla security and updates across a portfolio, see our Joomla agency handbook.

Frequently Asked Questions

What is the JCE Free/Pro 2.9.99.5 security update?

JCE Free/Pro 2.9.99.5 is a security release issued on 3 June 2026 that fixes insufficient access controls which let unauthenticated users upload editor profiles. Because an Editor Profile defines which filesystem and upload actions are permitted, the developer notes the flaw could be exploited to upload arbitrary files to the server. It affects all versions of JCE Free and JCE Pro before 2.9.99.5.

Is the JCE 2.9.99.5 vulnerability exploitable without a login?

Yes. This is the key difference from the 2.9.99.4 release a week earlier. The 2.9.99.4 bugs required an authenticated Joomla session. The 2.9.99.5 flaw does not. An anonymous visitor with no account could upload an editor profile, which is why this release should be applied to every Joomla site running JCE regardless of whether it allows registration.

Is JCE 2.9.99.5 the same bug as 2.9.99.4, or a different one?

It is a separate flaw. JCE 2.9.99.4 fixed two authenticated issues in the file browser: an Editor Profile access check and a directory traversal in filesystem search. JCE 2.9.99.5 fixes the access control on the profile upload action itself, and that one is unauthenticated. They appear to come from the same review of JCE's profile and filesystem code, but the changelog describes two distinct vulnerabilities, not a reopened 2.9.99.4.

Which JCE versions are affected by the 2.9.99.5 advisory?

All versions of JCE Free and JCE Pro prior to 2.9.99.5, including the entire 2.9.99.x branch and every older release. 2.9.99.5 is the first version with the fix in place. Long-tail installs that were never updated are equally at risk, and older branches carry their own backlog of unpatched issues on top of this one.

Has a CVE been assigned to the JCE 2.9.99.5 vulnerability?

No CVE number had been assigned at the time of writing. The absence of a CVE does not lower the severity. The vendor describes an unauthenticated path to uploading arbitrary files, which is treated as critical regardless of whether a CVE identifier exists yet.

How does mySites.guru help with the JCE 2.9.99.5 update?

mySites.guru indexes every extension on every connected Joomla site. The extension search lists every site with JCE installed, grouped by version, so you can find outdated

installs in seconds. The mass updater then pushes 2.9.99.5 across every affected site in one batch instead of logging into each administrator panel by hand.

Does this advisory affect WordPress?

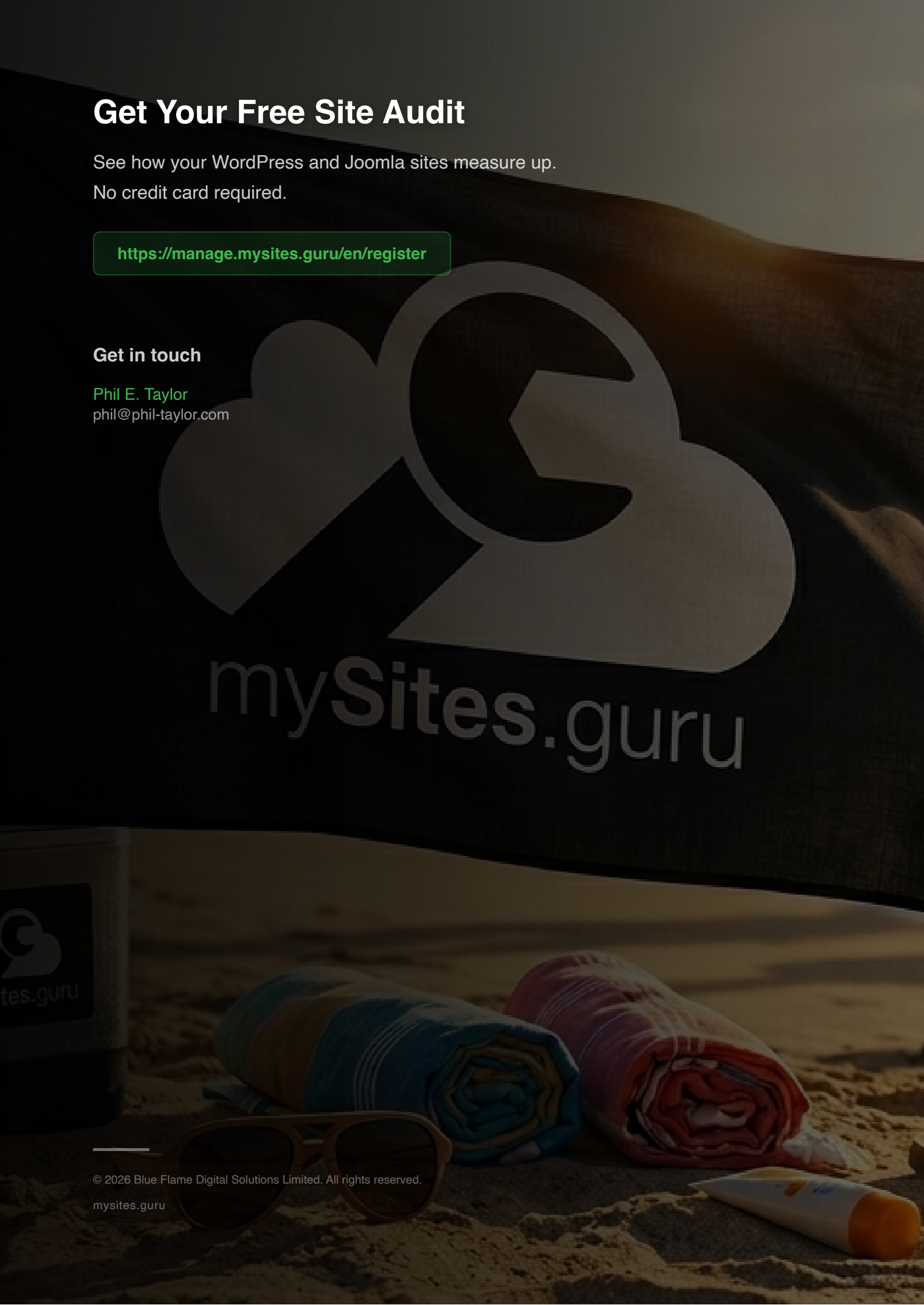
No. JCE is a Joomla-only editor extension. There is no WordPress build and no shared codebase. WordPress sites running the core block editor or TinyMCE are unaffected by this advisory.

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