mySites.guru

Fabrik for Joomla Fixes an Unauthenticated RCE in 4.6.7

Fabrik for Joomla up to 4.6.6 lets an anonymous visitor run code on your server through the calc element's AJAX endpoint. CVE-2026-66915, CVSS 10.0. Fixed in 4.6.7.

Phil E. Taylor | 10 August 2026

Active Joomla Extension security alerts: SP Page Builder zero day • Gridbox: 23 critical • JCE 2.9.99.10

Fabrik is an application builder for Joomla. You use it to construct forms, database-backed lists and small applications inside a Joomla site, and it has been on the Joomla Extensions Directory since 2014 with the project itself dating back to 2006. On 9 August 2026 its developers released **Fabrik 4.6.7** and labelled it a security release. The following morning the Joomla CNA published **CVE-2026-66915**, an **unauthenticated remote code execution** flaw in the extension's calc element, scored **CVSS 4.0 10.0 Critical**.

Every version from 1.0.0 through 4.6.6 is affected. That is the whole history of the extension. If you run Fabrik on any Joomla site, update it to 4.6.7 now. The complication, and the reason this is more than an afternoon's update run, is which of your sites can actually install it.

> **Update Fabrik to 4.6.7**
>
> Fabrik 4.6.7 is the fix, released 9 August 2026. Update every Joomla site running Fabrik. The update comes through Joomla's own updater or by direct download from the Fabrik site, and both require a valid Fabrik subscription. Fabrik 4.6.7 installs on Joomla 4.2 and above and Joomla 5.1 and above only, so sites on Joomla 3 or Joomla 6 need a different plan.

TL;DR

TL;DR: Fabrik's calc element computes a field value by evaluating a PHP expression that the site builder writes. When the element's AJAX option is on, that recalculation happens live through a front-end endpoint in `com_fabrik`, and that endpoint could be reached by an anonymous visitor with no login and no user interaction. Because evaluating PHP is the element's intended job, reaching it without authorisation means running code on the server. It is **CVE-2026-66915**, **CWE-94 code injection**, **CVSS 4.0 10.0 Critical** (`AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H`), reported by **Moe Khalilov of LeetProtect Research** and published by the Joomla CNA on 10

August 2026. Versions **1.0.0 to 4.6.6** are affected and **4.6.7** fixes it. The fix installs on **Joomla 4.2 to 5.x only** and needs a **valid Fabrik subscription**, and there is **no patched release for the Fabrik 3.x line** that Joomla 3 sites run. mySites.guru lists every connected Joomla site running Fabrik and the version on each, so you can find the affected ones in one place.

What Is Wrong in Fabrik's Calc Element?

The calc element is a Fabrik field whose value is worked out rather than typed. A site builder writes a small PHP expression into the element's settings, for example to total two other fields or apply a tax rate, and Fabrik evaluates that expression to produce the value. Evaluating site-builder PHP is the documented, intended behaviour of the element, and it is why Fabrik can do the things people use it for.

The element has an option to recalculate over AJAX, so the value updates live as a visitor fills in a form instead of only when the page reloads. That option adds a second route to the same evaluation: a front-end endpoint in the `com_fabrik` component that takes the current form data, substitutes it into the stored expression, and evaluates the result. In the Fabrik source that is public, which is the older Joomla 3 line, the calculation reaches a plain PHP `eval()` at the end of both routes. Fabrik 4.x is distributed only to subscribers and its source is not published anywhere we could find, so the description here is drawn from the public Joomla 3 code plus the CVE record's own classification of CWE-94, rather than from reading the patched release.

The flaw is that the AJAX route was reachable by anyone. No login, no privileges, no user interaction, which is exactly what the CVSS vector records with `PR:N` and `UI:N`. Joomla's standard input filtering runs on the submitted data, but that filter exists to strip HTML and script tags for cross-site scripting purposes and does not neutralise PHP syntax. Because the substitution happens before the evaluation, submitted data that steps outside its expected position changes what actually gets executed.

This is the same shape of problem we wrote about in AJAX endpoints being a CMS security blind spot: a helper route added for front-end convenience, sitting beside a well-guarded main path, that never inherited the main path's checks.

Why we are not publishing an exploit

A fix exists and shipped before the CVE published. We have described the shape of the flaw and named the component, because you need that to understand the risk and decide what to do. We are not publishing the endpoint parameters, the substitution syntax or any working proof of concept. Nothing here is a recipe.

Which Fabrik Versions Are Affected?

The CVE record lists **1.0.0 through 4.6.6** as affected and **4.6.7** as fixed. In practice that means every Fabrik release ever made, across both the Fabrik 3.x line built for Joomla 3 and the Fabrik 4.x line built for Joomla 4 and 5.

Fabrik's own changelog is unambiguous about what 4.6.7 is:

> *"Fabrik Base Version 4.6.7 (2026-08-09) Fix, 2026-08-09: Security fix for calc element Notes: This is a security release, please update immediately."*

The announcement on the Fabrik forum, posted by a project administrator on the evening of 9 August 2026, says the same thing and adds the practical constraints:

> *"Fabrik 4.6.7 is available. This is a security fix addressing the calc element. Please update immediatly. [...] You may download this update through the Joomla Updater or by direct download via My Download Files from the Fabrik site. Note: You will require a valid subscription in order to download or update. Fabrik 4 will not install on Joomla 6"*

Credit where it is due. This is a clearly labelled, clearly dated security release with an explicit instruction to update, published in two places on the day it shipped. We have covered plenty of vendors who buried a serious fix under "improved input validation" in a changelog, and Fabrik did not do that here.

Note on the missing 4.6.6

The CVE names 4.6.6 as the last affected version, but Fabrik's public changelog goes straight from 4.6.5 on 29 July 2026 to 4.6.7 on 9 August 2026, with no 4.6.6 entry. We have seen 4.6.6 reported by a real site, so the build exists. We could not find a public explanation of what happened to it, and Fabrik has retracted a bad build before, so treat 4.6.6 as affected and move to 4.6.7 regardless.

How Serious Is This Really?

The Joomla CNA scored it **10.0 Critical** on CVSS 4.0, the maximum. The vector says the attack comes over the network, needs no privileges, needs no user interaction, and produces high confidentiality, integrity and availability impact both on the vulnerable component and on the wider system. That is the score to work from, and it is the score we are working from.

The honest nuance is about reach rather than severity. Reaching the flaw needs the site to publish a Fabrik form or list that an anonymous visitor can load, and that form needs a calc element with the AJAX option enabled. A Fabrik install used only behind a login, or one with no calc elements, is a smaller target than the score alone implies.

That nuance is close to useless as an operational filter, for two reasons. Public forms are the ordinary use of Fabrik, not an edge case, and a site builder who wanted a login-only tool would usually reach for something simpler. And there is no practical way to audit “does any published form on this site contain an AJAX-enabled calc element” across more than a handful of sites without opening every form on every site by hand. Treat every install below 4.6.7 as affected, because you cannot cheaply prove otherwise.

Nobody had reported exploitation in the wild when this post went out, hours after the CVE published, and there is no CISA Known Exploited Vulnerabilities entry. Neither of those is reassuring on its own. An unauthenticated flaw that ends in code execution is the profile that attracts mass scanning quickly, and Joomla extension flaws of exactly this class have gone from disclosure to automated exploitation inside a week several times this year.

How to Fix Your Joomla Sites Running Fabrik

1. **Find every site running Fabrik and check the version.** Anything below 4.6.7 is affected. The component shows as `com_fabrik` in Joomla's extension manager.
2. **Confirm the Fabrik subscription is current.** Both update routes, Joomla's updater and direct download, check it. This is worth doing first, because discovering a lapsed subscription halfway through an update run across several sites wastes an afternoon.
3. **Update to Fabrik 4.6.7.** Through Joomla's own updater on each site, or by installing the downloaded package.
4. **Deal with the sites that cannot take it.** See the next section. Unpublishing public Fabrik forms and lists reduces exposure while you decide, though it is a stopgap rather than a fix.
5. **Check exposed sites for compromise.** Updating stops the next attempt and tells you nothing about whether one already succeeded. An unauthenticated flaw leaves no failed logins and no audit trail. Look for administrator accounts you did not create, recently modified or unfamiliar PHP files, and scheduled tasks nobody added. Our post on finding rogue admin accounts across every Joomla site covers the account side, and reinfection through crontabs covers a persistence route people routinely miss.

Not Every Joomla Site Can Install Fabrik 4.6.7

This is the part that turns a straightforward update into a project. Fabrik's installation notes for 4.6.7 say it installs on **Joomla 4.2 and above, and Joomla 5.1 and above**. The forum announcement adds that **Fabrik 4 will not install on Joomla 6**. So the fixed release has a compatibility window of Joomla 4.2 to Joomla 5.x, and sites at either end of that window are stuck.

Below the window sit the Joomla 3 sites. They run the Fabrik 3.x line, whose last release was **3.10 in August 2021**. The calc element's AJAX evaluation path is present in that code, the `joomla3` branch of the public repository has had no commits since 2016, and we found no 3.10.1 or equivalent security release anywhere. There is no patched version for those sites to move to.

Above the window sit the Joomla 6 sites, which the vendor's own announcement rules out in one line.

Across the Joomla sites we manage, this splits the affected population roughly two to one against being able to fix it by updating:

Joomla version	Share of the Fabrik sites we see	Can install 4.6.7?
Joomla 2.5	Under 1%	No
Joomla 3	61%	No
Joomla 4	6%	Yes
Joomla 5	30%	Yes
Joomla 6	3%	No

About one in eight of the Joomla 5 sites was already on 4.6.7 within a day of release, which is a genuinely good response time. Of the sites still on an affected version, **roughly two thirds are on a Joomla version the fix does not support**. The single most common configuration we see is Fabrik 3.10 on Joomla 3.10, which is a site running the newest version each project ever shipped for that generation, and exposed anyway.

If you have sites in that position, there are three honest options and no comfortable ones. Remove Fabrik, if the application it powers can be retired or rebuilt. Move the site onto Joomla 4.2 to 5.x, which is the work you were putting off anyway and now has a deadline attached. Or accept the risk knowingly, with public Fabrik forms unpublished, which is a holding position rather than a solution. Joomla 3 has been end of life since August 2023, and this is the ordinary way that debt gets called in, through a third-party

extension whose vendor has moved on to the next Joomla generation. We have written before about what is realistically available to sites still on Joomla 3.

Finding Every Fabrik Install Across Your Joomla Sites

Doing this by hand means logging in to each Joomla site, opening the extension manager, searching for Fabrik and writing the version down. For one site that is two minutes. For fifty it is an afternoon you will not get back, and you will still not be certain you checked them all.

mySites.guru keeps a live inventory of every extension, template and framework on every connected Joomla and WordPress site. Search the extension inventory for Fabrik once and you get back every site running it, the version each one is on, and whether an update is available, on one screen. Sites running a version flagged on our vulnerable extension list are marked automatically, so a site that drifts onto an affected version later gets flagged without anyone remembering to look.

For this particular flaw the inventory answers the second question too. Because it records the Joomla version alongside the extension version, you can separate the sites that just need an update from the sites that need a migration decision, which is the split that actually determines how much work you are looking at.

If a site turns out to have been compromised, fix.mysites.guru is a fixed fee of £120 per incident, usually same day. Sites are screened before we commit, so you are not charged if it cannot be fixed, and non-subscribers get a free month. There is more on recovery in our Joomla hacked guide.

Fabrik Has Been a Target Before

Fabrik has carried three earlier CVEs, and the pattern is worth knowing if you have run it for a long time:

- **CVE-2010-1981**, a directory traversal in com_fabrik 2.0 allowing arbitrary file reads
- **CVE-2011-5004**, an unrestricted file upload in the CSV import model, fixed before 2.1.1
- **CVE-2018-10727**, a reflected cross-site scripting flaw through a hidden referrer field, affecting versions through 3.8.1

The Joomla Vulnerable Extensions List also carries a resolved entry for “fabrik 3.9, Various Issues”, published in May 2020 and fixed in 3.9.1. CVE-2026-66915 was not on the VEL when this post was written, which is normal for a CVE that published the same morning.

There is also a more recent one that never got a CVE at all. Fabrik 4.6.3, released on 25 February 2026, carries a changelog line reading simply “Security fix” with no further detail, under the same “This is a security release, please update immediately” note that 4.6.7 uses. Nothing was published about what it closed. That is worth knowing if you are the sort of person who skips point releases on an extension that seems to be ticking over quietly, because at least twice this year a Fabrik point release has been the security update.

The 2011 upload flaw is the one that left a mark. Several public auto-exploiter tools targeting `com_fabrik` are still sitting on GitHub, written years ago against that bug. They are irrelevant to this CVE, but they are a reminder that a Joomla extension with a long history and a shell-upload flaw in its past stays on scanners’ lists long after the flaw is fixed.

Further Reading

- CVE-2026-66915 record - the Joomla CNA’s published record, with the CVSS 4.0 vector and affected version range
- Fabrik changelog history - the vendor’s own release notes, where 4.6.7 is documented as a security release

- Fabrik 4.6.7 release announcement - the forum post with the compatibility and subscription requirements
- Joomla Vulnerable Extensions List - the official list of known-vulnerable Joomla extensions
- CWE-94: Improper Control of Generation of Code - the weakness class this flaw belongs to

Frequently Asked Questions

What is CVE-2026-66915?

CVE-2026-66915 is an unauthenticated remote code execution flaw in Fabrik, the application and form builder extension for Joomla. The calc element plugin evaluates a PHP expression to work out a field's value, and its AJAX recalculation endpoint could be reached by anyone with no login. An anonymous visitor could influence what that expression evaluated to, which meant running their own code on your server. The Joomla CNA published it on 10 August 2026 and scored it CVSS 4.0 10.0 Critical, classed as CWE-94 code injection. It was reported by Moe Khalilov of LeetProtect Research.

Which Fabrik versions are affected?

The CVE record lists every version from 1.0.0 through 4.6.6 as affected, which covers the entire history of the extension including the whole Fabrik 3.x line for Joomla 3. Fabrik 4.6.7, released on 9 August 2026, is the fix. There is no patched release on the Fabrik 3.x branch, whose last version was 3.10 in August 2021.

Can I install Fabrik 4.6.7 on my Joomla 3 site?

No. Fabrik's own installation notes for 4.6.7 say it installs on Joomla 4.2 and above, and Joomla 5.1 and above. The vendor's release announcement also states that Fabrik 4 will not install on Joomla 6. So the fixed version has a compatibility window of Joomla 4.2 to Joomla 5.x, and sites on Joomla 3 or older, or on Joomla 6, cannot install it. For those sites the practical options are removing Fabrik or moving the site onto a Joomla version the fix supports.

Do I need a Fabrik subscription to get the fix?

Yes. Fabrik's release announcement says plainly that a valid subscription is required in order to download or update. The update is delivered either through Joomla's own updater or by direct download from the Fabrik site, and both routes check the subscription. A site with a lapsed subscription cannot pull 4.6.7, which is worth checking before you plan an update run across several sites.

How do I know if my Joomla site is exposed?

Exposure depends on whether the site publishes a Fabrik form or list that a visitor can reach without logging in, and whether any element on it is a calc element with AJAX recalculation enabled. That is difficult to audit by hand across more than a couple of sites, and the CNA scored the flaw as needing no privileges and no user interaction, so the sensible assumption

is that any install below 4.6.7 is affected until it is updated. mySites.guru lists every connected Joomla site running Fabrik with the version on each, so you can see the whole set at once instead of logging in to each site.

Is CVE-2026-66915 being exploited in the wild?

There were no public reports of exploitation and no CISA Known Exploited Vulnerabilities entry when this post was written, on 10 August 2026, hours after the CVE published. That is what you would expect this early and it is not a reason to relax. The flaw needs no account, works over a normal web request and ends in code running on the server, which is the profile that attracts mass scanning quickly once details circulate.

What is the Fabrik calc element for?

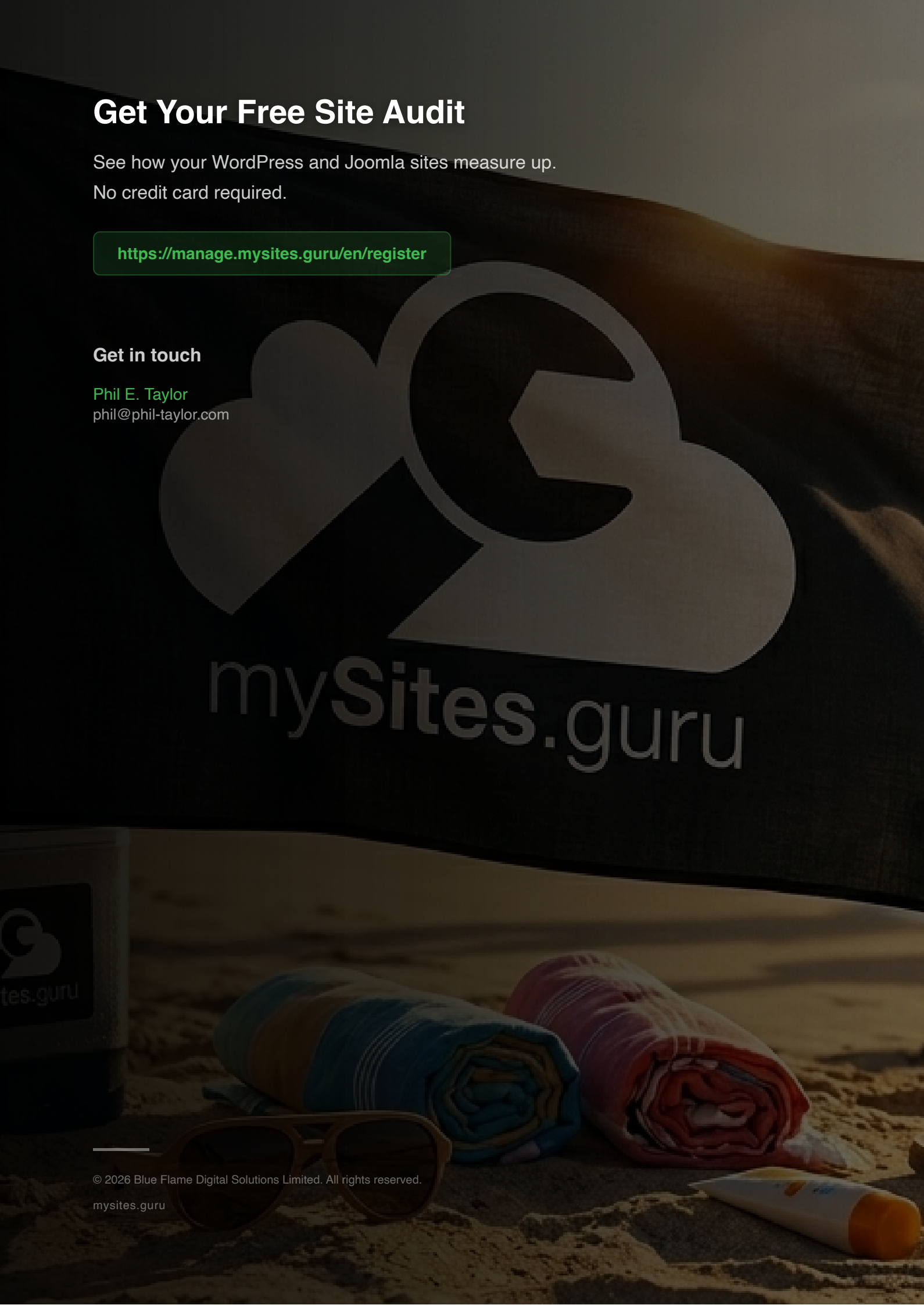
Fabrik is an application builder, so it lets you construct forms and database-backed lists inside Joomla. The calc element is a field whose value is worked out by a PHP expression that the site builder writes, for example totalling two other fields or applying a tax rate. The AJAX option makes that recalculation happen live as a visitor types, without reloading the page. Evaluating site-builder PHP is the element's intended job, which is why a flaw in how it is reached becomes code execution rather than a data leak.

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