mySites.guru

J2Commerce 6.6.6 Stops One Gift Voucher Paying for Several Orders

J2Commerce 6.6.6 fixes CVE-2026-102803, a checkout race that let one gift voucher or single-use coupon pay for several orders. Who is affected, what to do.

Phil E. Taylor | 10 November 2026

TL;DR

J2Commerce, LLC released J2Commerce 6.6.6 on 7 November 2026 with a fix for a security issue it named only by its identifier, CVE-2026-102803. The Joomla CNA published the record on 10 November 2026, and it describes a checkout race. In J2Commerce 6.0.0 to 6.6.5, a logged-in customer could open several checkouts at once, take each one to the confirm step, and then submit them all. Every one of those orders saw the gift voucher's full balance, or the single-use coupon's one unused slot, so a single voucher could pay for several orders.

J2Commerce is a Joomla e-commerce extension, so this is a flaw in the extension and Joomla itself is not involved. The cost is the shop's money: no data is read and the site is not taken over. It needs a customer account, and a guest cannot do it. The record credits no researcher, the flaw is not in CISA's Known Exploited Vulnerabilities list, and no one has said it was exploited. Update to 6.6.6, then check recent orders for a voucher or coupon code that appears more than once.

6.0
CVSS 4.0

CVE-2026-102803 J2Commerce 6.0.0 to 6.6.5: one gift voucher or single-use coupon redeemed on several orders

MEDIUM **Joomla CNA (CVE record)**

A logged-in customer who opens several checkouts at once can spend one gift voucher's full balance, or one single-use coupon, on each of those orders.

`CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N`

Customer account needed | Concurrent checkouts | Shop revenue, not data

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

`AV:N` Network: Reachable across the internet
`AC:L` Low: Nothing to work around, it just works
`AT:P` Present: Needs a particular deployment or race to line up
`PR:L` Low: Any logged-in account will do
`UI:N` None: Nobody has to be tricked into anything

What it does to the site

`VC:N` None: Nothing can be read
`VI:H` High: Data and files can be altered at will
`VA:N` None: The site stays up

What it does beyond the site

`SC:N` None: Other systems keep their data
`SI:N` None: Other systems keep their integrity
`SA:N` None: Other systems stay up

What the CVE Record Says About J2Commerce 6.6.6

The CVE-2026-102803 record was reserved on 29 September 2026 and published by the Joomla CNA on 10 November 2026. Its title is “Gift voucher and single-use coupon could pay for more than one order in J2Store 6.0.0 - 6.6.5”, and its description sets out the mechanism in two sentences.

The CNA's description of CVE-2026-102803, in full

A logged-in customer could redeem a single gift voucher, or a single-use coupon (`max_uses` / `max_customer_uses` = 1), on more than one order. By starting several checkout sessions and carrying each to the confirm step before submitting any of them, every order independently saw the voucher’s full balance or the coupon’s unused slot, because the balance/usage calculations and the final placement check both only looked at orders that had already left the “New” state.

The naming needs one note. The record calls the product “J2Store extension for Joomla”, from the vendor j2commerce.com, and gives the range as J2Store 6.0.0 - 6.6.5. The 6.x line is sold and installed as J2Commerce 6, and its component is com_j2commerce, so this post says J2Commerce throughout. If you search for the CVE and find J2Store in the title, it is the same flaw and the same fix.

The vendor said much less. The J2Commerce 6.6.6 release post has this and no more on the subject: “J2Commerce 6.6.6 includes a fix for a security issue tracked as CVE-2026-102803. Updating to 6.6.6 applies the fix”. It gives no class of flaw, no severity and no affected range. All three came from the CVE record three days later, which is why a shop owner who read the release post on the day had no way to judge how urgent the update was.

How One Gift Voucher Paid for Several J2Commerce Orders

A gift voucher is a balance. When a customer applies one at checkout, the shop works out how much of it is left by adding up what earlier orders have already spent, and offers the remainder against the new order. A single-use coupon works the same way with a count in place of a balance: the shop counts the orders that have used the code and rejects it once the limit is reached. The record’s `max_uses` and `max_customer_uses` settings are those limits, and a value of 1 is what makes a coupon single-use.

The flaw is in which orders got counted. According to the record, the balance and usage calculations only looked at orders that had already left the “New” state. An order that a customer has built and taken to the confirm step, but not yet submitted, is still in that state. As far as the sums were concerned, it had spent no money yet.

So a logged-in customer could do this:

1. Open several checkout sessions at once, in separate browser tabs for example.
2. Apply the same gift voucher, or the same single-use coupon, in each.
3. Take each checkout as far as the confirm step and stop there.
4. Submit them one after another.

At step 3, each checkout asked how much of the voucher was left, and each got the same answer: all of it, because none of the other orders had left “New”. The record says the final placement check, the last look before an order is accepted, used the same

rule, so it did not catch the overlap either. Each order was approved on its own, against a balance that the others were about to spend as well.

In plain terms, a gift voucher worth a given amount could pay for several orders, each up to that full amount. A coupon meant for one use could discount several orders. The record files this under CWE-367, a time-of-check time-of-use race condition: the shop checked the balance at one moment and relied on it at a later one, and the answer had changed in between.

Why the score is Medium

The Joomla CNA scores it 6.0 Medium under CVSS 4.0, with the vector CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N. It is reachable over the network with low complexity and no interaction from anybody else. Two metrics hold the score down. PR:L, low privileges, is the customer account: the record says “logged-in customer”, so a guest checkout is not enough. AT:P, attack requirements present, is the timing: several checkouts have to be open and waiting at the confirm step together.

The impact metrics describe the kind of damage. Integrity is High, because orders are accepted against money that was not there. Confidentiality and availability are both None. No customer data is read, the attacker gets no access to the Joomla administrator, and the shop keeps running. What goes missing is revenue, in goods shipped against a voucher that had already been spent.

A Medium score is a fair reading of the general case, and a shop that sells gift vouchers should still treat it as money it may already have lost. The two requirements are a customer account and a few checkouts open at once, and neither takes any skill.

Which J2Commerce Versions and Joomla Sites Are Affected?

J2Commerce 6.0.0 to 6.6.5 are affected, and 6.6.6 is the fixed version. J2Commerce 6 runs only on Joomla 6 and needs PHP 8.3, as covered in the J2Store 3 end of life post,

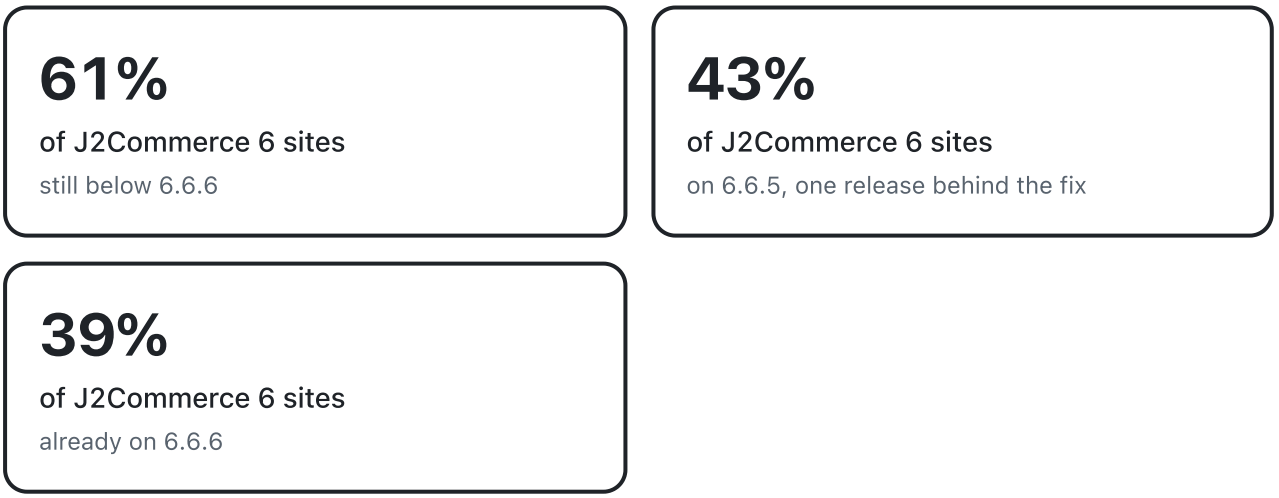
so an affected shop is always a Joomla 6 site.

Version	Component	Status	What to do
J2Commerce 6.6.6	com_j2commerce	Fixed	Check recent orders
J2Commerce 6.0.0 to 6.6.5	com_j2commerce	Affected	Update to 6.6.6
J2Store 3.x and 4.x	com_j2store	Not named by this CVE	Nothing for this CVE

The older J2Store 3.x and 4.x lines are a separate component, com_j2store, and CVE-2026-102803 does not name them. They have had their own problems, written up in the post on six more J2Store flaws, but this record is about the 6.x line only.

One more limit comes from the flaw itself. A shop that sells no gift vouchers and has no coupons with a usage limit gives an attacker no way in through this flaw. It should still update, because the next person to create a single-use coupon on that shop will not be thinking about this CVE.

On the afternoon the record was published, this is where the J2Commerce 6 sites in the mySites.guru database stood:



J2Commerce 6 sites in the mySites.guru database on the afternoon of 10 November 2026.

On 9 November 2026, two days after the release, about 4% of those sites were on 6.6.6. A day later it was 39%. Most of the sites still behind were on 6.6.5, the release

immediately before the fix, so for most of them the fix is a single update away. The oldest installs were on the 6.3 line.

What To Do on a J2Commerce Shop Now

1. Update J2Commerce to 6.6.6. No setting in 6.0.0 to 6.6.5 turns the race off, so the update is the fix.
2. Look through recent orders for the same gift voucher code on more than one order, and do the same for any single-use coupon code. Orders placed close together by the same customer are the pattern the record describes.
3. Check each gift voucher's balance against the orders that used it. A voucher that has paid out more than it was worth has been spent more than once.
4. If you look after several J2Commerce shops, update them in one pass and then do steps 2 and 3 on the ones that sell gift vouchers or run limited coupons.

Steps 2 and 3 matter even though no one has reported exploitation. The update stops it happening again, and it does not tell you whether it already has. A shop on 6.x has had the flaw since 6.0.0, and a customer who stumbled on it with two tabs open would not have announced it.

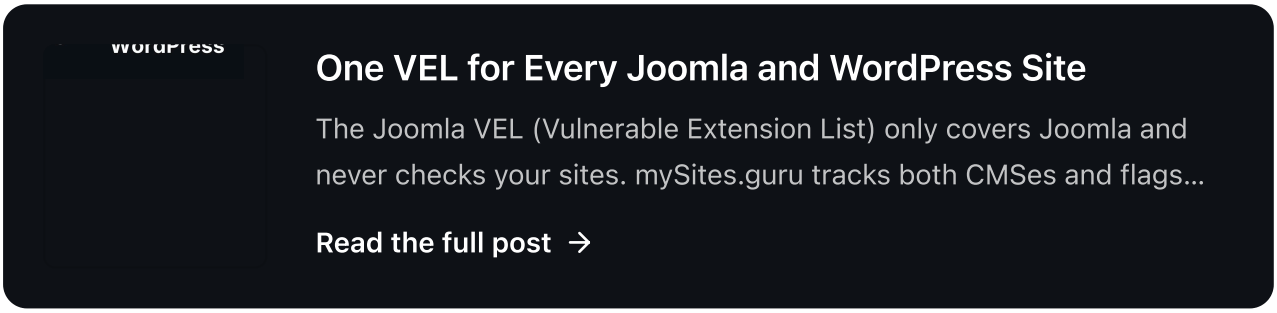
This release also shows what a vendor's one-line security note leaves you with. For three days the only public statement was that 6.6.6 fixed a security issue, with no word on whether it was minor or serious. Shops that apply extension updates as they arrive did not need to know. The guide to enabling Joomla extension auto-updates covers how to set that up and which extensions it is sensible for.

How mySites.guru Flags J2Commerce

On 9 November 2026, before the details were public, we added a rule that flags every connected Joomla site running the J2Commerce component below 6.6.6. The vendor's release post was enough to act on: it named a CVE and a fixed version, and a site below that version was missing a security fix whatever the flaw turned out to be. When the

record was published on 10 November 2026 we updated the rule with the published range, 6.0.0 to 6.6.5, and the Medium severity. The rule has its own page at CVE-2026-102803.

Flagged sites appear in the vulnerable extension list with their installed version, so you can see at a glance which shops are on 6.6.5 and which are further back. The mass updater then bulk updates Joomla extensions across many sites in one run, which is how a group of shops goes from 6.6.5 to 6.6.6 without anyone logging in to each one. Every rule we hold is on the public vulnerabilities page, and the flags and the updater are part of the subscription.



This flaw costs a shop money without anyone breaking into the site. For a site that has been hacked, fix.mySites.guru patches it, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Timeline

2026-09-29 — **CVE-2026-102803 reserved**
The Joomla CNA reserves the identifier.

2026-11-07 — **J2Commerce 6.6.6 released**
J2Commerce, LLC announces 6.6.6 with a fix for a security issue tracked as CVE-2026-102803, with no further detail.

2026-11-09 — **mySites.guru flags affected sites**

A rule flags every connected Joomla site on J2Commerce below 6.6.6, before the details are public.

2026-11-10

CVE record published

The Joomla CNA publishes the record: gift voucher and single-use coupon reuse across concurrent checkouts, CVSS 4.0 6.0 Medium, J2Store 6.0.0 - 6.6.5.

Further Reading

- CVE-2026-102803 - the Joomla CNA's record, with the description, the affected range and the CVSS 4.0 vector.
- J2Commerce 6.6.6: new features and updates - the vendor's release post, which names the CVE and the fixed version.
- J2Store 3 End of Life - the older J2Store line, and what J2Commerce 6 needs from Joomla and PHP.
- Six more J2Store flaws - an earlier disclosure covering the same family of Joomla shop extensions.

Frequently Asked Questions

Which J2Commerce version fixes the gift voucher and coupon reuse flaw?

J2Commerce 6.6.6, released by J2Commerce, LLC. Versions 6.0.0 to 6.6.5 are affected. Older versions have no setting that switches the flaw off, so the update is the fix.

Is there a CVE for the J2Commerce 6.6.6 fix, and how severe is it?

Yes, CVE-2026-102803, published by the Joomla CNA. The CVSS 4.0 base score is 6.0 Medium and the weakness class is CWE-367, a time-of-check time-of-use race condition. The record credits no researcher, and the flaw is not in CISA's Known Exploited Vulnerabilities list.

Does someone need a customer account to reuse a voucher on a J2Commerce shop?

Yes. The CVE record describes a logged-in customer, and the score records low privileges, which here means a customer account. The customer also has to open several checkouts at once and take each one to the confirm step before submitting any of them.

Does CVE-2026-102803 affect J2Store 3 or J2Store 4?

The CVE names versions 6.0.0 to 6.6.5 only. The record calls the product J2Store, but the 6.x line is sold and installed as J2Commerce 6, component com_j2commerce. The older J2Store 3.x and 4.x lines are a separate component, com_j2store, and this CVE does not name them.

How do I check whether a gift voucher or coupon was used more than once?

After updating to 6.6.6, look through recent orders for the same gift voucher code or single-use coupon code on more than one order. Then check each gift voucher's balance against the orders that used it. A voucher that paid for more than its value is the sign.



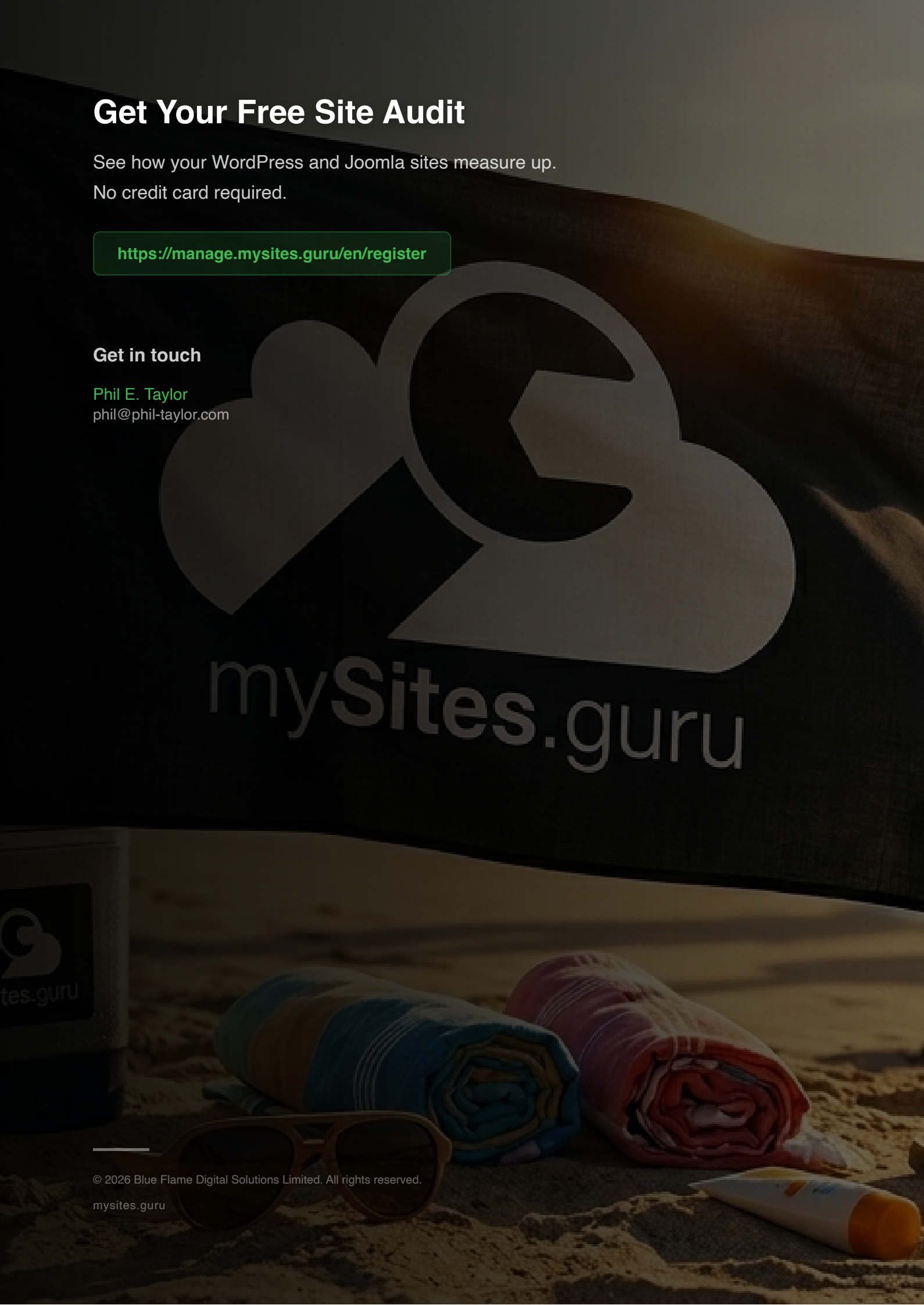
Written and edited by a human, with AI assistance. Our approach to AI

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

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.