mySites.guru

CVE-2026-105296: Akeeba Fixed These CSRF Gaps in July

Akeeba fixed the CSRF gaps behind CVE-2026-105296 on 30 July 2026, in Akeeba Backup 10.3.7 and Admin Tools 7.9.0. JPCERT/CC published the CVE in November.

Phil E. Taylor | 4 November 2026

A CVE dated 4 November 2026, CVE-2026-105296, appeared today in vulnerability feeds and scanners for Akeeba Backup and Admin Tools. It describes a set of cross-site request forgery gaps that Akeeba found while auditing its own code and fixed on 30 July 2026, in the releases described in its news post of that day. The affected versions in the record are Akeeba Backup for Joomla before 10.3.7 and Admin Tools for Joomla before 7.9.0 (Akeeba Backup for WordPress and Akeeba Solo before 9.1.8 are also named).

If you have updated Akeeba Backup and Admin Tools at any point since July, there is nothing to do. If you have not, this is a good reason to catch up, and the rest of this post is about why a fix from the summer has a CVE from the autumn, and how to read one when it turns up.

What to do

Update Akeeba Backup for Joomla to 10.3.7 or later and Admin Tools for Joomla to 7.9.0 or later. Any current release is fine. The CVE range also covers the older Joomla 3 lines (Akeeba Backup 8.x and earlier, Admin Tools 6.x and earlier). We have not seen a fixed release on those lines, so on Joomla 3 the fix is migrating.

5.1
CVSS 4.0

CVE-2026-105296 Cross-Site Request Forgery in Akeeba Backup and Admin Tools

MEDIUM **JPCERT/CC (CNA)**

A logged-in administrator tricked into visiting a malicious page could trigger some low-impact backend actions.

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

▼ 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:N` None: Works against any affected install
`PR:N` None: No account needed
`UI:A` Active: Someone has to be talked through a few steps

What it does to the site

`VC:L` Low: Some data can be read
`VI:L` Low: Some data can be altered
`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

TL;DR

- CVE-2026-105296 is a cross-site request forgery (CSRF) issue in Akeeba Backup for Joomla before 10.3.7, Admin Tools for Joomla before 7.9.0, and Akeeba Backup for WordPress and Akeeba Solo before 9.1.8
- Akeeba found the gaps in its own audit and fixed them on 30 July 2026, explaining the fix in plain words the same day
- The CVE was reserved on 5 October 2026 and published on 4 November 2026 by JPCERT/CC, Japan's CERT, which is a CVE Numbering Authority in its own right. It did not come from the Joomla CNA or the Joomla Security Strike Team
- A CSRF attack needs a logged-in administrator to be tricked into visiting a malicious page. Akeeba's own worst case is deleting an offsite copy of a backup archive, with no path to running code, reading data or taking over an account
- No exploitation is on record: Akeeba says it has no indication of any, and the CISA assessment on the record says exploitation none
- Across the Joomla sites connected to mySites.guru, 86.5% of installs on the current Akeeba Backup line were already on 10.3.7 or later on the day the CVE was published

- mySites.guru flags every connected Joomla site still on an affected version, including the Joomla 3 lines

What Akeeba fixed in July

Cross-site request forgery works like this. You are logged into your site's administrator in one tab. In another tab you open a page an attacker controls. That page makes your browser send a request to your own site, and because your browser attaches your login cookie, the site treats it as yours. The usual defence is an anti-CSRF token: a secret the site puts in its own forms, which a page on another domain cannot know. An action that does not check for the token can be triggered by a forged request.

Akeeba's 10.3.7 release notes list the Akeeba Backup actions that now require the token: the backup filter, exclusion and inclusion editors; deleting and downloading archives stored remotely; the Transfer Wizard, Upload and S3 import flows; the FTP and SFTP connection tests; the Configuration Wizard; and some minor control panel actions. The same day's releases of Akeeba Backup for WordPress 9.1.8, Akeeba Solo 9.1.8 and Admin Tools 7.9.0 made the equivalent changes.

Every one of those actions was already restricted to a logged-in administrator of the extension. Akeeba's notes also point out that most of them are submitted in a way that current browsers' default cookie policy (SameSite) already blocks from cross-site use, so on a modern browser most of the gaps were already closed before the code changed. Akeeba's own worst case, from the news post: a logged-in user tricked into deleting an offsite copy of a backup archive in Akeeba Backup or Solo, if the attacker also knows that archive's ID, or into running the temporary directory cleaner in Admin Tools. Some of the other affected features would just open an unexpected page and sit there waiting for the user to do something. There was no path to running code, reading your data, or taking over an account.

Akeeba described the issues as low severity, said it had no indication any of them were exploited, and released the changes as a precaution and as defence in depth. The same releases also tidied up some access-control inconsistencies that only matter if you had chosen to delegate access to lower-privileged users (the default is Super User only),

and Admin Tools 7.9.0 added new security features, among them the return of UploadShield. That is a well-handled hardening release from a vendor auditing its own software, which is the behaviour you want from the people who look after your backups.

Why does a July fix have a November CVE?

Because a CVE is a record, and this record was opened by a different organisation, on a different timeline, from the one Akeeba worked to. JPCERT/CC, Japan's computer emergency response team, is a CVE Numbering Authority (CNA): an organisation allowed to assign CVE ids within its scope. The Joomla CNA, run by the Joomla Security Strike Team, is the one most Joomla extension users know, but it is not the only CNA that can issue a CVE for a Joomla extension. Any CNA can, within its scope.

The route here is visible in JVN#44272550, the Japanese vulnerability note published alongside the CVE on 4 November 2026. Kuniyoshi Noguchi reported the issue in Akeeba Backup for Joomla to IPA, and JPCERT/CC coordinated with Akeeba under its Information Security Early Warning Partnership. The note then says something that is easy to skim past: the developer had found the vulnerability independently of the report and was progressing to release each fixed version. The outside report and Akeeba's own audit found the same gaps, and Akeeba's fixes were already on their way out.

The dates on the record follow from that. The CVE id was reserved on 5 October 2026, more than two months after the fixed versions came out, and published on 4 November 2026, 97 days after Akeeba's news post. Neither date tells you when the issue was fixed. A CVE's published date is the day its record went public.

In our view, a CVE arriving three months after the vendor released and explained the fix can sound more alarming than the issue was. The record's CVSS 4.0 score of 5.1 Medium (5.4 Medium on CVSS 3.0) is a generic severity assessment, and Akeeba's own notes give the practical picture, which is a logged-in administrator being tricked into a low-impact action. None of that is a criticism of the reporter or of JPCERT/CC. CVE records for already-fixed issues are normal and useful, because a tool like ours can only flag what has an identifier. Read the record with the fix date beside it.

How to read a CVE that arrives after the fix

A CVE that turns up months after the update is common, and agencies looking after many sites need a quick way to size one up. This is the check we ran on CVE-2026-105296, and it is the one to run on the next one.

1. Find the fix date before the CVE date. Here the fix came out on 30 July 2026 and the record was published on 4 November 2026. If your sites updated in between, the CVE is a label for something you already dealt with.
2. Read the vendor's own notes. Akeeba's news post and release notes say which actions were affected, what the worst case was, and that none of it could get a site hacked. A CNA record describes the weakness class; the vendor describes what it meant on a real site.
3. Read the vector, not just the score. The vector `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N` includes `PR:N` and `UI:A`: no privileges needed by the attacker, but active user interaction required. For a CSRF issue that means a logged-in administrator has to be tricked into visiting a page. An outsider cannot trigger it against a site without that administrator.
4. Check the exploitation status. The CISA ADP assessment attached to the record on 4 November 2026 says exploitation none, automatable no, technical impact partial, and the CVE is not in the CISA Known Exploited Vulnerabilities catalogue. Akeeba says it has no indication of exploitation either.
5. Then update anyway, on your normal schedule rather than at 2am. Nothing above is a reason to stay on an old version.

How many Joomla sites were already patched?

Most of them. We checked the Akeeba Backup and Admin Tools versions across the Joomla sites connected to mySites.guru on 4 November 2026, the day the CVE was published, and the majority of sites had taken the July fix in the months before the record existed.

86.5%

Akeeba Backup already fixed

Installs on the current line (10.x, Joomla 4 and later) that were on 10.3.7 or later when the CVE was published. 96.2% are on a 10.x release.

89.9%

Admin Tools already fixed

Admin Tools 7.x installs on 7.9.0 or later.

about a fifth

still on the Joomla 3 lines

21.4% of Akeeba Backup installs are the legacy Joomla 3 line (8.x and older); 22.7% of Admin Tools installs are pre-7.

mySites.guru connected Joomla sites, 4 November 2026.

A security update that a vendor releases and explains clearly gets taken up quickly by sites that update at all, so the CVE changes little for the typical Akeeba customer. It matters most for the sites that stopped updating, and for the fifth or so still on the Joomla 3 lines, where we have not seen a fixed version to update to.

Joomla 3 sites on older Akeeba Backup and Admin Tools

The CVE range is “before 10.3.7” for Akeeba Backup for Joomla and “before 7.9.0” for Admin Tools for Joomla, which takes in the legacy com_akeeba line (Akeeba Backup 8.x and older) and Admin Tools 6.x and older that Joomla 3 sites run. Akeeba’s July releases were for the current lines, we have not seen a fixed Joomla 3 release since, and Akeeba’s Joomla 3 position is on record. A site on Joomla 3 with the old Akeeba Backup or Admin Tools installed will stay flagged for this CVE until it migrates to a current Joomla and a current Akeeba release.

The practical risk on those sites is the same as described above, a logged-in administrator being tricked into a low-impact action, so it is one more item on the list of reasons a Joomla 3 site needs a migration plan rather than an emergency on its own.

How mySites.guru flags CVE-2026-105296

As of 4 November 2026, every Joomla site connected to mySites.guru that runs Akeeba Backup below 10.3.7 (the current com_akeebabackup line and the legacy com_akeeba line both) or Admin Tools below 7.9.0 is flagged with this CVE in its extension list and in its vulnerability alerts. The rule and the affected range are on the CVE-2026-105296 page, one of the entries in our public vulnerability list, and the Joomla vulnerability scanner page explains how the extension inventory behind it works.

For an agency with many sites, the useful view is the one across all of them: which sites are still on an affected version, grouped by the update that fixes it. On current Joomla sites that is an Akeeba Backup or Admin Tools update you can push from the bulk update screen; on Joomla 3 sites it is a migration. Either way, if you updated Akeeba Backup since July, you were fixed before this CVE existed, and the record is a label on work you already did.

Timeline

2026-07-30

Akeeba ships the fixes

Akeeba Backup for Joomla 10.3.7, Akeeba Backup for WordPress 9.1.8, Akeeba Solo 9.1.8 and Admin Tools for Joomla 7.9.0 are released together, with a news post explaining the CSRF hardening found in Akeeba's own audit.

2026-10-05

CVE id reserved by JPCERT/CC

More than two months after the fixed versions came out, JPCERT/CC reserves CVE-2026-105296 for the same CSRF gaps, following a report to Japan's IPA.

2026-11-04

CVE-2026-105296 published, rules added the same day

The CVE record and JVN#44272550 are published. mySites.guru adds a rule the same day, flagging every connected Joomla site on Akeeba

Backup below 10.3.7 or Admin Tools below 7.9.0.

Further Reading

- Security Hardening in Today's Akeeba Backup, Solo, and Admin Tools Releases - Akeeba's 30 July 2026 news post, the plain-words account of what was fixed and what it could and could not do.
- Akeeba Backup 10.3.7 release notes - the list of actions that now require an anti-CSRF token.
- JVN#44272550 - the Japanese vulnerability note behind the CVE, with the credit and the coordination summary.
- CVE-2026-105296 at cve.org - the CNA record, affected versions and both CVSS scores.
- CWE-352: Cross-Site Request Forgery - the weakness class.
- Joomla extension updates can now be flagged as security releases - how a security update shows up differently from a routine one in mySites.guru.

Frequently Asked Questions

Is my site at risk if it already runs Akeeba Backup 10.3.7 or Admin Tools 7.9.0?

No. Akeeba Backup for Joomla 10.3.7 and Admin Tools for Joomla 7.9.0, both released on 30 July 2026, are the fixed versions named in the CVE record. Any later release is fixed too. There is nothing extra to do for this security issue on a site that took those updates.

Why did I get an alert about CVE-2026-105296 now, months after the fix?

The CVE id was reserved on 5 October 2026 and published on 4 November 2026 by JPCERT/CC, so it only existed as a record from November. Vulnerability tools, mySites.guru included, flag sites by the record. Akeeba released and explained the fix on 30 July 2026. A site still on an older version is flagged because it missed that update, not because anything changed on the site.

Was this security issue exploited?

Akeeba's release notes say there is no indication any of the issues were exploited, and the CISA ADP assessment attached to the CVE record on 4 November 2026 records exploitation as none. The CVE is not in the CISA Known Exploited Vulnerabilities catalogue.

Did the Joomla Security Strike Team issue CVE-2026-105296?

No. It was assigned and published by JPCERT/CC, Japan's CERT, which is a CVE Numbering Authority in its own right. A report went to Japan's IPA, JPCERT/CC coordinated with Akeeba, and JVN notes that Akeeba had already found the issue on its own and was releasing fixed versions. The Joomla CNA is not the only CNA that can issue a CVE for a Joomla extension.

What about Joomla 3 sites on the older Akeeba Backup 8 or Admin Tools 6 lines?

The CVE range covers every Akeeba Backup for Joomla release before 10.3.7 and every Admin Tools for Joomla release before 7.9.0, which includes the legacy Joomla 3 lines. Akeeba's July releases were for the current lines, and we have not seen a fixed release on the Joomla 3 lines since. The fix for a Joomla 3 site is to migrate it to a current Joomla and a current Akeeba release.



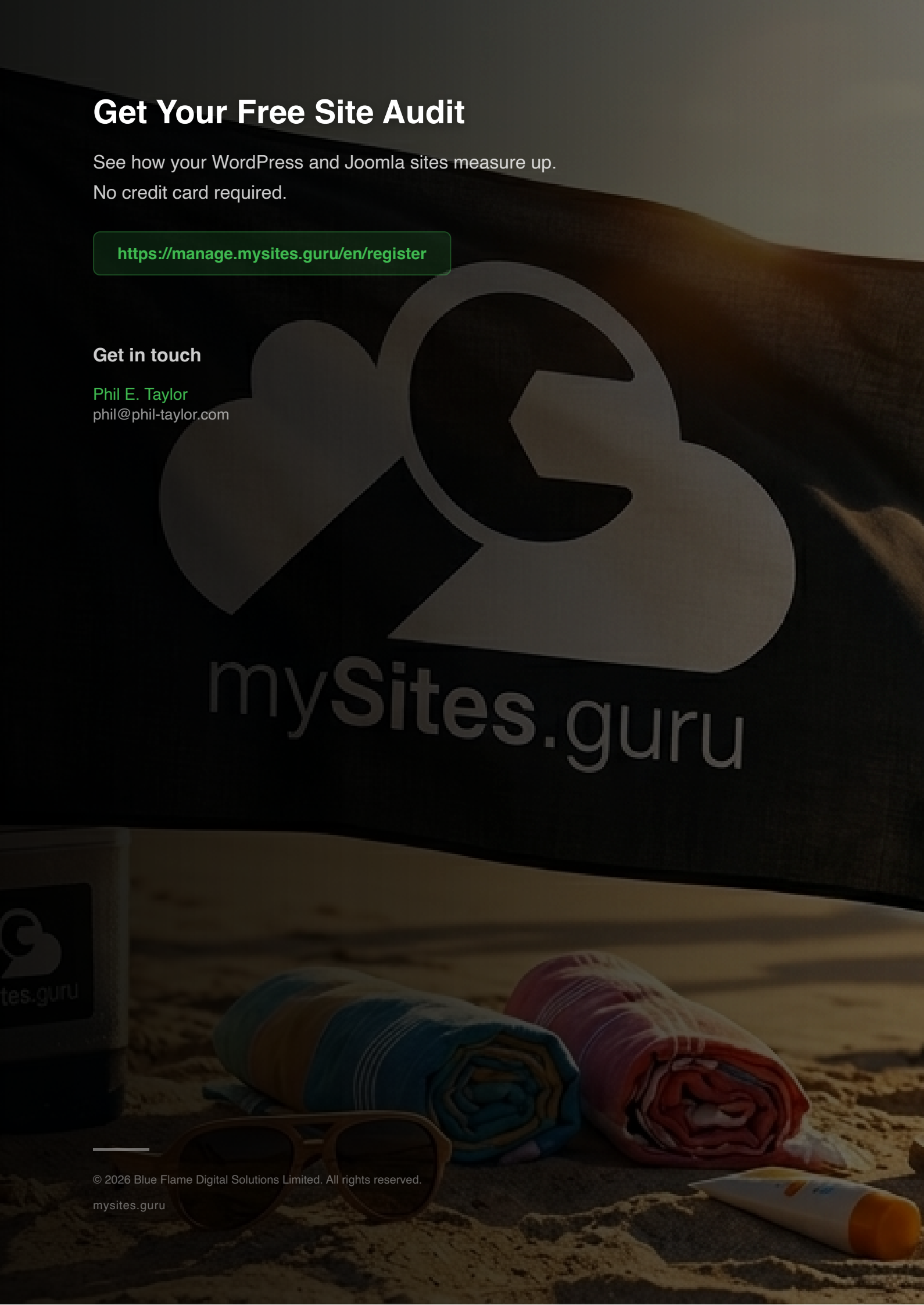
Written and edited by a human, with AI assistance. Our approach to AI

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.