



14 More Joomla 3 Security Fixes, Each Tested on a Real 3.10.12 Site

Joomla 5.4.9 fixed 16 core issues. We backported every one reaching Joomla 3 to the mySites.guru one-click patch tool, each proved on a real 3.10.12 site.

Phil E. Taylor | 2 October 2026

Joomla's September 2026 release, Joomla 5.4.9 and 6.1.4, closed sixteen core security issues. If you run a Joomla 3 site, you will never be offered a single one of them. Joomla 3 reached end of life in August 2023 at version 3.10.12, and the project ships security fixes only for Joomla 5 and 6.

There used to be a paid way to keep getting them. Joomla's Extended Long Term Support programme backported fixes to Joomla 3 for a subscription, but it ended on 17 February 2025 and has shipped nothing since. So as of 2025, there is no official source of new Joomla 3 core security fixes at all, paid or free.

That is the gap our one-click Joomla 3 patch tool fills, and this month it grew. We backported the nine September fixes that reach Joomla 3, found five more from the spring that had slipped past us, and shipped all fourteen. The tool went from 65 files to 85.

The short version

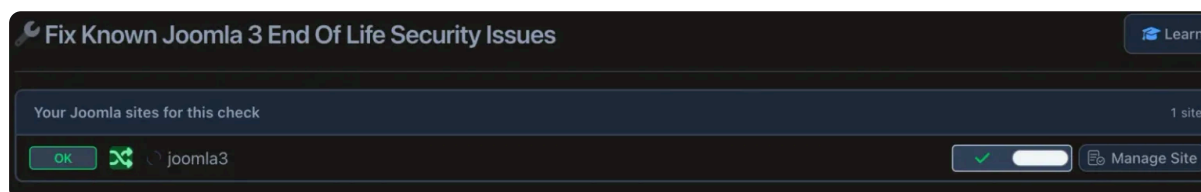
Fourteen more Joomla core security fixes are now in the mySites.guru one-click Joomla 3 patch tool, every one of them reproduced on a real Joomla 3.10.12 install before we shipped it. One toggle patches all 85 files. No eLTS subscription, and switch it off to revert.

What does the mySites.guru Joomla 3 patch tool do?

The tool is a toggle in each Joomla 3.10.12 site's Snapshot. Flip it on and the mySites.guru connector compares the hash of every file that needs patching against the version we ship, replacing anything that does not match. Flip it off and the files revert to stock 3.10.12. There is nothing to upload, no eLTS licence, and no risk of being stranded on a half-applied patch.

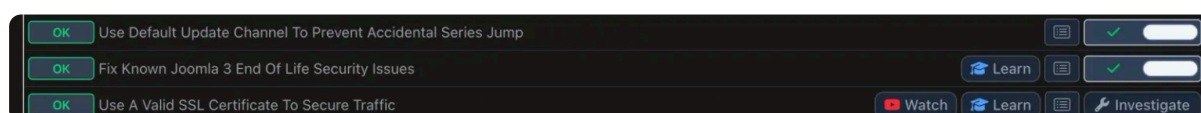
The patch goes on top of official Joomla 3.10.12, nothing else

It patches the official Joomla 3.10.12 files. It is not a patch on top of an eLTS build, or a third-party fork such as JoomlaWorks' unofficial Joomla 3.x "up to date" (which continues Joomla 3 under its own version numbering), or any other Joomla 3 series. If your site runs an eLTS release, a fork, or any version other than stock 3.10.12, upload the full fresh official Joomla 3.10.12 files over the site first, then run the tool to patch them. Straight from official 3.10.12 to the mySites.guru patch is the only supported path.

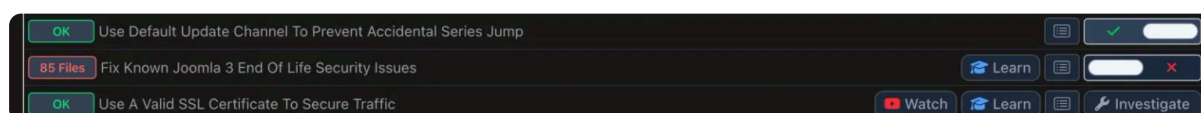


The tool lists every Joomla 3 site in your account with its own toggle, so you can patch one site or the whole list from one page.

Each Joomla 3 site also shows the same check as a row in its Snapshot. A green OK badge and an on toggle mean the site has every file in the current patch set. When the patch set grows, the badge turns red and shows how many files are now behind, so you know there is new protection to apply rather than having to go looking.



Patched: a green OK badge and the toggle on, meaning every file matches the current patch set.



Not patched: a red badge showing 85 files behind, after the October 2026 update grew the set. One toggle applies all of them.

Under the hood the patches come from the open-source [Joomla 3.10.999 project](#), the same approach as the earlier [Joomla 1.5.999](#) and [Joomla 2.5.999](#) repositories. The how-to linked above has the full walkthrough of where the tool lives and how to patch sites in bulk. This post is about what went into it in October 2026, and how we decided.

What Joomla fixed in 5.4.9, and what reaches Joomla 3

Of the sixteen core issues in Joomla 5.4.9, nine reach the Joomla 3 code and are now patched. The other seven live in parts of Joomla that version 3 never had: the webservice API endpoints, the workflow engine, the HTML mail templates. There is no Joomla 3 equivalent to patch, so they are simply out of scope rather than ignored.

Four of the nine are worth describing, because they are the kind of flaw that sits unnoticed on an end-of-life site until someone goes looking:

- **A guest could create a user account (CVE-2026-90907).** The `profile.save` controller never checked whether the person calling it was logged in, so a signed-out visitor could create a guest-level account even on a site with user registration turned off. The fix rejects a guest outright.
- **Arbitrary directory deletion through the cache (CVE-2026-90915).** The file cache did not properly validate a cache group name, so a crafted name with `../` in it could walk out of the cache folder and delete directories elsewhere. The patched version resolves the path and rejects anything that escapes the cache root.
- **Server-side request forgery (CVE-2026-92222).** Several URL fields accepted any scheme, so a URL meant to point at a feed could be pointed at an internal service instead. The fix restricts those fields to `http` and `https`.
- **Two XSS filter bypasses (CVE-2026-92231 and CVE-2026-92232).** Joomla's input filter could be tricked into keeping a `javascript:` URL by hiding it behind an HTML5 entity, or a `data:text/html` payload behind a tab character. Both are now decoded and stripped the way a browser would read them.

The full list, with every advisory link, is in the [one-click how-to](#).

Why we don't trust the "affected versions" field

This is where the real work is. A Joomla advisory lists the versions it affects, and the obvious thing to do is read that field and patch the versions it names. We don't,

because the field is written against the versions Joomla still supports, and the vulnerable code is often older than the oldest version listed.

Four of September's advisories are rated "Joomla 4.0 and later": the cache directory-deletion above, two improper-ACL checks on tagged items and the content-history comparison view, and an XSS in the module list. Read the field literally and you would skip all four on Joomla 3. Read the actual 3.10.12 source and the same flawed code is right there.

So we reproduce each candidate on a stock Joomla 3.10.12 install before it goes in. We stand up a real site, write a test that triggers the flaw, confirm it fires on the unpatched files, apply the backported fix, and confirm the test now fails to trigger it while the legitimate behaviour still works. The cache directory-deletion and both ACL checks earned their place in the Joomla 3 set that way, not because an advisory told us to add them.

The spring 2026 fixes came out of the same discipline. While checking the September batch against 3.10.12 we noticed five earlier ones that reach Joomla 3 and had never been added: an XSS in the feed modules, an XSS in `com_contenthistory`, a local file inclusion in a layout parameter, and two more input-filter hardening fixes. They are in now too.

The fix we left out on purpose

One September advisory did not make the cut, and that is the point of being precise. CVE-2026-21629 is an ACL hardening fix for `com_ajax`, and it is rated as affecting Joomla 3. But on Joomla 3 the administrator application sends every signed-out visitor to the login screen before `com_ajax` ever runs. The vulnerable path is not reachable, so there is nothing to patch.

We could have added the file anyway and claimed a bigger number. Inflating the count would make the tool look more thorough while doing nothing for a single site. A patch set is only worth trusting if every file in it is there for a reason, so a CVE that cannot fire on Joomla 3 stays out, and this post tells you which one and why.

How many files does the Joomla 3 patch tool change?

The tool now touches 85 files: 43 PHP files that hold the actual fixes, 37 XML form definitions that tighten input validation, three language files and two CA certificate bundles. Eighty-four are replaced with patched versions and one is a file Joomla 3 never shipped, created when you toggle on and deleted when you toggle off.

Because the patch set ships with the connector, it grows as new Joomla 3 CVEs are backported, and a site that was fully patched then reads as behind until you re-toggle. That is the mechanism doing its job, not a regression: the connector only counts a file as patched when it matches the exact version we ship today, so “fully patched” always means current, never current as of some fixed date.

What to do if you still run Joomla 3

Start planning the new site on a modern Joomla version. Patching Joomla 3 is a holding action, not a plan: the PHP it runs on, the extensions built for it, and the tooling around it are all aging out, and no amount of core patching saves you long term. A fresh build on Joomla 5 is the only real fix, so get it on the roadmap now rather than when something breaks.

For the sites you cannot, will not, or do not want to move yet, [patch them](#). Switch the toggle on, and if you manage many Joomla 3 sites the bulk view patches them together. The case for keeping these sites covered while you plan their future is in [Joomla 3 Didn't Fail. Your Retainer Did.](#)

This tool patches every known Joomla 3 core security issue

One toggle, 85 files, every Joomla core vulnerability we have confirmed reaches Joomla 3.
No eLTS subscription, and reversible at any time.

Core is not the only thing aging on a Joomla 3 site. The extensions are [going end of life alongside it](#), which is why we also patch [JoomShaper's Helix and SP Page Builder](#)

separately. Between the two, the known holes come off the table while you do the real work of migrating.

Further reading

- [Joomla 6.1.4 and 5.4.9 Security and Bugfix Release](#) - Joomla's own announcement of the September 2026 release the backport is based on.
- [Joomla Security Centre](#) - the official advisory feed, where every CVE in the patch set is published.
- [The Joomla 3.10.999 project](#) - the open-source repository the patches come from.
- [Fix Joomla 3 Security Issues in One Click](#) - the full how-to, including the complete file and CVE list and the bulk view.
- [Joomla Extended Long Term Support \(eLTS\)](#) - the paid programme that patched Joomla 3 until it ended on 17 February 2025.

Frequently Asked Questions

How many security fixes are in the mySites.guru Joomla 3 patch tool now?

The tool patches 85 files, covering every Joomla core vulnerability disclosed since 3.10.12 that we have confirmed reaches the Joomla 3 code. The October 2026 update added 14 more fixes: the nine from Joomla's September release (5.4.9) that apply to Joomla 3, plus five from spring 2026 that we found had been missed while we were working through the new batch.

Why does mySites.guru patch CVEs that Joomla says only affect Joomla 4 and later?

Because the affected-versions field in a Joomla advisory is not always the full story. Four of the September 2026 advisories are rated 'Joomla 4.0 and later', but the same flawed code is in Joomla 3.10.12. We reproduce each one on a stock 3.10.12 install before deciding, so the patch set is based on what the code actually does, not on which versions the advisory happens to list.

Do I have to do anything to get the new Joomla 3 fixes?

After the connector update ships, your Joomla 3 sites will show as not fully patched on the next snapshot, because the patch set grew. Switch the one-click toggle on (or off and on again if it was already on) to apply the new files. There is nothing to install and no eLTS subscription to buy.

Is every September Joomla CVE now in the Joomla 3 patch tool?

Every one that reaches Joomla 3 is, which is nine of the sixteen in Joomla 5.4.9. The others are in Joomla 4, 5 or 6 code that Joomla 3 never had, such as the webservice API endpoints and the workflow engine, so there is nothing to patch on a Joomla 3 site. We also left out CVE-2026-21629 on purpose, because Joomla 3 already blocks the request it concerns before the vulnerable code runs.

Does the patch tool work on any Joomla 3 site?

It works on any Joomla 3.10.12 install, the last public release of the Joomla 3 series. The connector compares the file hashes on your site against the patched versions and replaces anything that does not match. Flip the toggle off and the files revert to stock 3.10.12, so it is fully reversible.

What if I'm running an eLTS version or a Joomla 3 version other than 3.10.12?

The patch applies on top of the official Joomla 3.10.12 files only. It is not a patch on top of an eLTS build, a third-party fork such as JoomlaWorks' unofficial 'Joomla 3.x' (which continues Joomla 3 under its own version numbering), or any other Joomla 3 series. If your site runs one of those, upload the full fresh official Joomla 3.10.12 files over the site first, then run the mySites.guru tool to patch them. Going straight from official 3.10.12 to the mySites.guru patch is the only supported path.

Is patching Joomla 3 a substitute for migrating to Joomla 5?

No. The patch closes known core security holes so a site that cannot migrate today is not left exposed, but Joomla 3 is end of life and its PHP support, extensions and tooling keep moving on without it. Treat the patch as cover while you plan the move to Joomla 5, not as a reason to stay.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

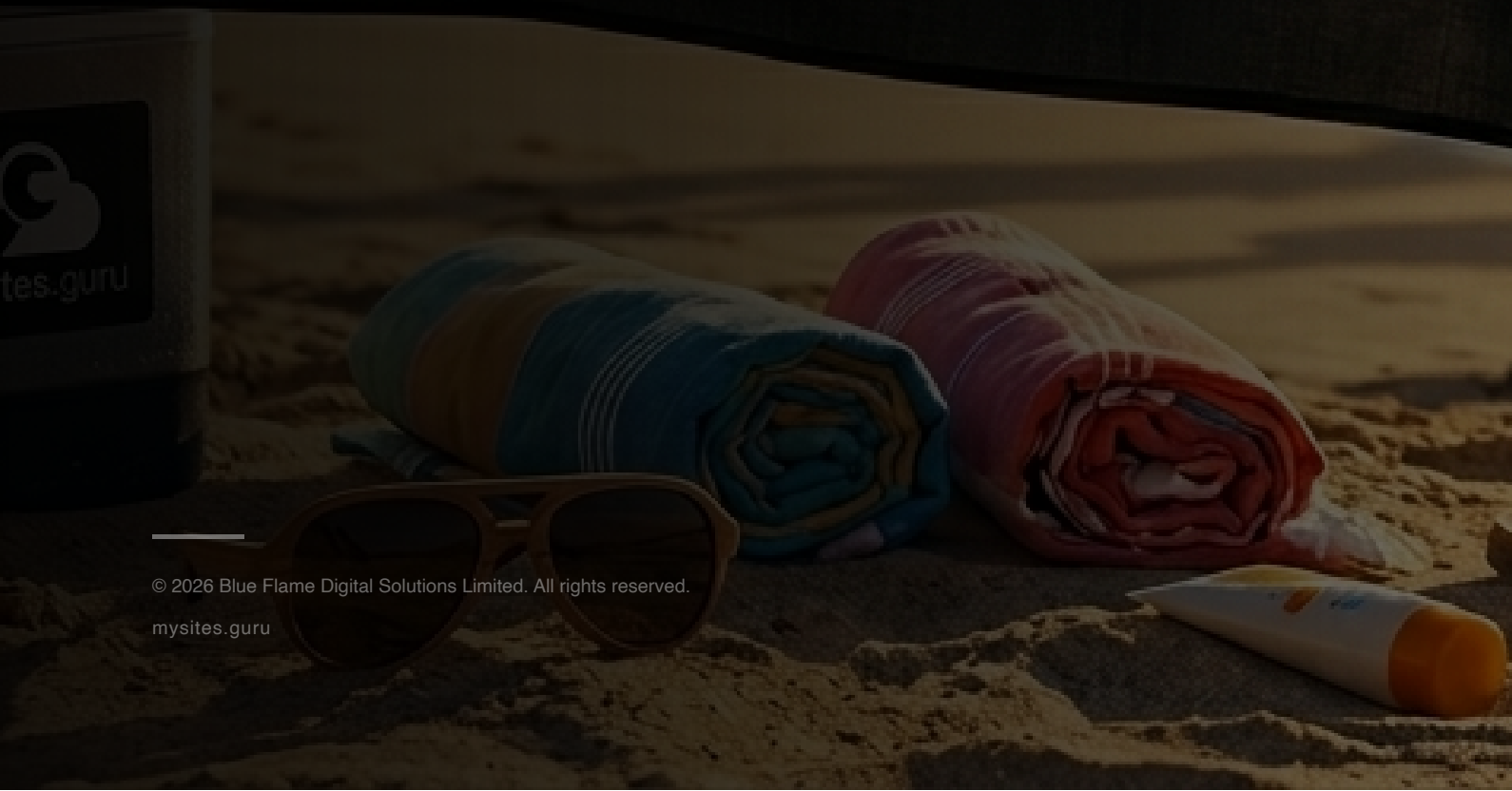
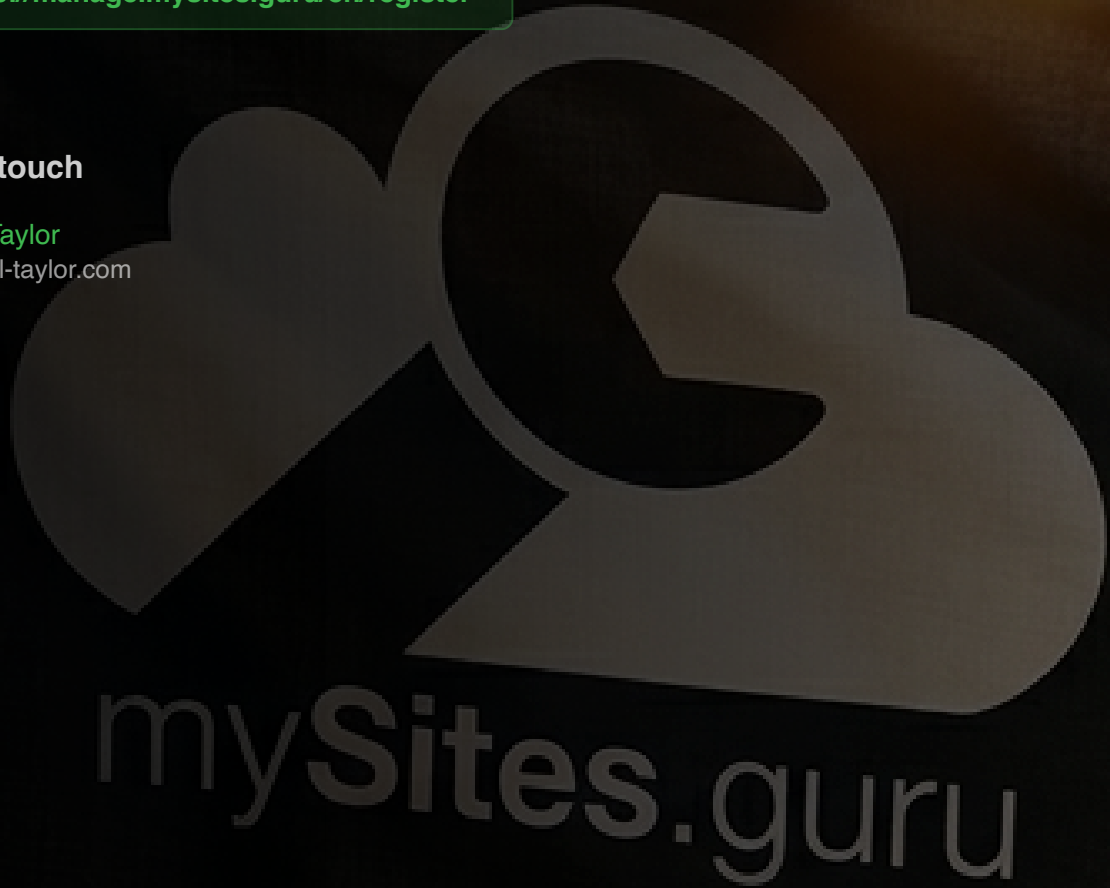
Get Your Free Site Audit

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.

mysites.guru