



# JoomShaper Ends Joomla 3 Security Fixes

JoomShaper has stopped patching Joomla 3 versions of SP Page Builder, Helix and its other products. No security fixes, regardless of severity. What to do about it.

Phil E. Taylor | 9 July 2026



**Active Joomla security alerts: [Helix3 File Write](#) · [JCE Profiles Hack](#) · [PageBuilder CK RCE](#) · [Balbooa Forms RCE](#) · [SP Page Builder Zero Day](#)**

JoomShaper, the developer behind SP Page Builder and the Helix framework, has stopped supporting Joomla 3. In [an announcement on 9 July 2026](#) the company confirmed that the Joomla 3 versions of all its products now get no updates, and one line stands out: "No security patches, regardless of severity." If a critical flaw turns up in the Joomla 3 build of SP Page Builder tomorrow, it does not get fixed.

That is a defensible decision, and JoomShaper explains it well: they can secure their own code, but "we can't secure the Joomla core underneath it," and the Joomla 3 core has been end of life for a long time. The problem is not the decision. The problem is how many live sites this leaves exposed, and how recently JoomShaper's own extensions have produced exactly the kind of flaw this policy now leaves unpatched.

**"No security patches, regardless of severity."**

**JOOMSHAPER, ON JOOMLA 3 SUPPORT, 9 JULY 2026**

## What JoomShaper Actually Announced

JoomShaper has ended support for the Joomla 3 versions of every product it makes. That covers SP Page Builder, the Helix framework (both Helix Ultimate and the older Helix3), EasyStore, Power Admin, and its Joomla templates. The Joomla 4, 5, and 6 builds of these products are unaffected and still supported. Only the Joomla 3 versions are frozen.

The policy is blunt on purpose. No feature updates, no compatibility fixes, and no security patches “regardless of severity” for the Joomla 3 builds. JoomShaper’s stated reasoning is that patching its own extension does nothing when the platform beneath it, the Joomla 3 core, no longer receives fixes either. That is true, and it is the honest position. It also means a Joomla 3 site running these extensions now has two unpatched layers instead of one.

One clarification worth making, because it gets muddled: Gantry is not a JoomShaper product. Gantry is a RocketTheme framework, and this announcement does not touch it. If you run Gantry-based templates, this specific news is not about you, though the wider Joomla 3 end-of-life problem still is.

## Why This Is Worse Than a Normal End-of-Life Notice

Here is the editorial connection JoomShaper did not make, and it is ours, not theirs. Following a disastrous month of security issues for their products, they are freezing Joomla 3 support just as the risk to those products is at its most visible. SP Page Builder had a critical remote code execution flaw exploited in the wild, and the Helix framework produced two more serious issues in the same window. Now the Joomla 3 builds of exactly those products get no more fixes.

In June 2026, SP Page Builder had an unauthenticated file upload vulnerability, [CVE-2026-48908](#), scored CVSS 10.0, the maximum. It let anyone on the internet upload and run a file with no login, and it was used in the wild to plant hidden Joomla Super User accounts. JoomShaper fixed it promptly in version 6.6.2. That fix reached Joomla 4, 5, and 6 sites. Under the policy announced this week, the equivalent fix for a Joomla 3 site would not exist.

This is not hypothetical. SP Page Builder and Helix are among the most widely installed Joomla extensions in the world, precisely the kind of large, front-facing code that keeps producing this class of bug. A vulnerability of the same severity will turn up again. When it does, Joomla 3 sites are on their own.

## How Many Sites Does This Affect?

More than half of all live Joomla sites. According to [W3Techs](#), as of July 2026 Joomla 3 still accounts for 54.3 percent of every Joomla site online, the single largest share by version. Joomla 5 sits at around 20 percent, Joomla 4 under 10, and Joomla 6 is still in the single digits.

That number is the whole story. This is not a niche announcement affecting a handful of legacy holdouts. It is a policy change that lands on the majority of the Joomla web, most of which also runs SP Page Builder or Helix because those are the tools people built Joomla 3 sites with in the first place. If you manage Joomla sites for clients, the odds are high that some of them fall in exactly this gap.

## How Do I Find Every Joomla 3 Site I Manage?

The first job is knowing your exposure, and doing it by hand does not scale. Logging into each site to check its Joomla version and installed extensions is fine for three sites and impossible for thirty. You need one screen that shows every site, its Joomla version, and which JoomShaper extensions each one runs.

mySites.guru keeps a live inventory of every Joomla and WordPress site in your account, with the core version and the full extension list for each. You can filter for Joomla 3 sites in seconds, then cross-reference which of them run SP Page Builder or Helix, so you know which sites are in the danger zone rather than guessing. It also **flags end-of-life versions automatically**, so an unsupported core shows up as a warning without you going looking for it.

Find your Joomla 3 exposure in one place

[Open your Extension Inventory](#)

Filter for Joomla 3 sites and search for SP Page Builder or Helix to see which sites are exposed. Not a subscriber? [Sign up free](#) and connect your sites.

## Can I Keep a Joomla 3 Site Patched While I Migrate?

Yes, as a stopgap for the core, but not forever and not for the extensions. There are two separate holes to think about: the Joomla 3 core, and the vendor extensions on top of it.

For the core, mySites.guru can apply the [Joomla 3.10.999 project's backported security patches with a single toggle](#). That project quietly backported the critical fixes that landed in Joomla 4 to end-of-life Joomla 3 sites, so a site with the toggle on has the known core holes closed. It is the closest thing to keeping an unsupported core safe, and it does not need an eLTS subscription or any manual file edits.

### Patch every known Joomla 3 core issue in one click

mySites.guru applies the backported Joomla 3.10.999 security patches across all your Joomla 3 sites from one screen. It buys you time to migrate. [See how the one-click Joomla 3 fix works.](#)

What the core patch cannot do is fix an extension the vendor has abandoned. If a new SP Page Builder or Helix flaw appears on Joomla 3, no toggle backports a fix that JoomShaper has chosen not to write. That is the line between a stopgap and a solution. Keeping the core patched is sensible while you plan; leaving a Joomla 3 site on SP Page Builder patches indefinitely is not.

## The Real Fix Is Migration

Patching is a holding pattern. The actual answer to an end-of-life core and an end-of-life vendor policy is to get off Joomla 3, and the supported targets are Joomla 5 and Joomla 6. Note that Joomla 4 is not a safe destination either: its own security support ended in October 2025, so migrating from 3 to 4 would land you on another unsupported line. Aim for 5 or 6 directly.

Migration is real work, and the honest framing is that it takes planning rather than a click. The part that trips agencies up is keeping sites connected to their management

tooling through the version jump. mySites.guru's connector handles that, so a site stays monitored and backed up right through the migration rather than dropping off your dashboard mid-move. The [migration walkthrough](#) covers the connector swap step by step.

Before you touch anything, take a full backup, and ideally test the migration on a staging copy first. A Joomla 3 site with SP Page Builder content has a lot of layout data that needs to survive the jump, and you want to find any problems on a copy, not on the live site.

## This Is Part of a Wider Pattern in Joomla Extensions

JoomShaper freezing Joomla 3 is not an isolated event. It sits inside a run of critical Joomla extension flaws we have documented over recent weeks, and the common thread is unauthenticated file uploads leading to remote code execution. The same class of bug turned up in [PageBuilder CK](#), [iCagenda](#), and [Balbooa Forms](#), and JoomShaper's own Helix framework had [a critical fix shipped quietly as a plain "Security Update"](#) that then fed [a defacement wave stored in the database](#), alongside a separate [unauthenticated menu write in Helix Ultimate](#).

The lesson for anyone running Joomla at scale is that the extension layer is where the attacks land, and a Joomla 3 site now carries that risk with no vendor safety net on either the core or the biggest extensions. That is why the version you run matters as much as the extensions you install.

## The Bottom Line

JoomShaper has done the responsible thing by being clear rather than quietly letting Joomla 3 support rot, and "no security patches, regardless of severity" is at least honest. But it lands on more than half the Joomla web, weeks after their own SP Page Builder had a CVSS 10.0 flaw exploited in the wild. If you manage Joomla sites, find every Joomla 3 install you look after, confirm which run SP Page Builder or Helix, keep

the core patched as a stopgap, and move the priority sites to Joomla 5 or 6. Start with a free audit on one site to see what your Joomla 3 exposure actually looks like.

## Further Reading

- JoomShaper: Ending Joomla 3 Support - the original vendor announcement, including the "no security patches, regardless of severity" policy.
- Joomla End of Life dates (endoflife.date) - a live reference for which Joomla versions are still supported and when each line reaches end of life.
- Joomla Extended Security Support (eLTS) - the official Joomla project programme that patched Joomla 3 until it ended on 17 February 2025.
- W3Techs Joomla version usage - the current breakdown of live Joomla sites by version, showing how much of the web still runs Joomla 3.
- CVE-2026-48908 - the SP Page Builder unauthenticated file upload record, the flaw that makes this policy change bite.

# Frequently Asked Questions

## What did JoomShaper announce about Joomla 3?

On 9 July 2026 JoomShaper announced it has stopped supporting Joomla 3 across all its products, including SP Page Builder, the Helix framework, EasyStore, Power Admin, and its templates. The key line is that Joomla 3 versions of these products now receive no security patches, regardless of severity. JoomShaper's reasoning is that it can secure its own code but cannot secure the end-of-life Joomla core underneath it.

## Which JoomShaper products are affected?

The Joomla 3 builds of SP Page Builder, Helix Ultimate, Helix3, EasyStore, Power Admin, and JoomShaper's Joomla templates. The Joomla 4, 5, and 6 versions of these products are unaffected and continue to be supported. Note that Gantry is a RocketTheme framework, not a JoomShaper one, so it is not part of this announcement.

## Is Joomla 3 itself still supported?

No. Joomla 3.10 reached end of life on 17 August 2023. The official paid Extended Long Term Security Support (eLTS) programme then patched it until 17 February 2025, and that has now ended too. Since February 2025 there have been no official security patches for the Joomla 3 core, of any severity.

## How urgent is this for my Joomla 3 sites?

Treat it as urgent if any Joomla 3 site you manage runs SP Page Builder or Helix, because those are large, internet-facing extensions that have produced critical remote code execution flaws recently. SP Page Builder had an unauthenticated file upload flaw (CVE-2026-48908, CVSS 10.0) actively exploited in June 2026. Under the new policy, the next flaw of that kind on a Joomla 3 site would not be patched by the vendor.

## What should I do about my Joomla 3 sites now?

Two things, in order. First, find every Joomla 3 site you manage and which JoomShaper extensions each one runs, so you know your exposure. Second, plan migration to Joomla 5 or 6. Patching buys time, but migration is the only real fix. mySites.guru finds every Joomla 3 site in your account, flags the end-of-life versions, keeps them patched while you plan, and helps you migrate.

## Can I still patch a Joomla 3 site if I cannot migrate immediately?

Yes, as a stopgap. mySites.guru can apply the backported Joomla 3 core security patches from the 3.10.999 project with a single toggle, which closes the known core holes while you schedule migration. It does not fix a vendor extension that the vendor has stopped patching, so any Joomla 3 site running SP Page Builder or Helix should be migrated as a priority, not left on patches indefinitely.


# 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



mySites.guru

---

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

mysites.guru