



SP Page Builder's Joomla 3 Security Patch Was Incomplete. Version 1.0.3 Fixes It.

JoomShaper's first Joomla 3 security patch for SP Page Builder left the captcha bypass live and the XSS fix incomplete. Version 1.0.3 closes both.

Phil E. Taylor | 2 October 2026

JoomShaper has released version 1.0.3 of the Joomla 3 Security Patch for SP Page Builder, and it finishes a job the first release started. When SP Page Builder 6.9.1 fixed five security issues we reported, Joomla 3 sites were left out, because they cannot run the 6.x package at all. The Joomla 3 patch that shipped alongside it, version 1.0.2, was meant to back-port those fixes. It back-ported four of them, left the fifth live, and shipped a cross-site scripting fix that stopped one character short. Version 1.0.3 closes both gaps.

We found them while verifying the released packages on 14 September, proved each on a Joomla 3.10.12 test site with the patch files in place, and reported them to JoomShaper the same day. This post is what those two gaps were, how 1.0.3 addresses them, and the part that no patch version fixes: most Joomla 3 sites running SP Page Builder cannot install it.

What version 1.0.2 left open

The 6.9.1 round had five findings. Four of them are ordinary back-ports: the same corrected code, moved to the older files. The two that did not travel cleanly are the interesting ones, and both are the kind of gap that appears when a fix is applied to the exact place it was reported and not to the code sitting next to it.

The first was the captcha bypass. The second was an XSS fix that escaped one of two sinks on the same line. There was also a smaller observation about where the captcha type is read from, which 1.0.3 has now tidied up as well.

6.9

CVSS 4.0

CVE-2026-79701 Unauthenticated captcha bypass in the contact, form builder and opt-in form addons

MEDIUM

Joomla CNA, published 14 September 2026 and being extended to the Joomla 3 branch

An anonymous visitor gets past reCAPTCHA on any of the three Pro form addons by claiming the form sits inside a module. The 1.0.2 patch left this live on Joomla 3, and the opt-in form was not in the patch at all. Fixed in 1.0.3.

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

No login needed

Exploitable over the internet

Captcha not verified

Fixed in 1.0.3

▼ 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:N None: Nobody has to be tricked into anything

What it does to the site

VC:N None: Nothing can be read

VI:L Low: Some data can be altered

VA:L Low: The site slows or stutters

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

5.1

CVSS 4.0

CVE-2026-102426: reflected XSS in the dynamic content filter addon

MEDIUM

mySites.guru assessment. The Joomla CNA has assigned the id but not yet published a score

A crafted link to a page using the dynamic content filter prints the attacker's HTML into the page, so their script runs in the visitor's browser as your site. It needs someone to click the link, and it is worse

when that person is logged in as an administrator. Joomla 3 branch only. Fixed in 1.0.3.

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

No login needed

Victim must click a link

Reflected XSS

Joomla 3 only

Fixed in 1.0.3

▼ 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:N None: Nothing can be read

VI:N None: Nothing can be altered

VA:N None: The site stays up

What it does beyond the site

SC:L Low: Some data on other systems can be read

SI:L Low: Some data on other systems can be altered

SA:N None: Other systems stay up

The captcha bypass that never reached Joomla 3

SP Page Builder's Pro form addons verify their captcha in a public AJAX handler that anyone can call. The bypass, described in full in the 6.9.1 write-up, is that the handler reads a **view_type** value straight from the request, and when that value says the form is being rendered inside a module, the code throws away the real captcha result and replaces it with a test of whether the submitted token is merely non-empty. Declare **view_type=module** and the captcha is gone. It is published as CVE-2026-79701, with an affected range reaching back to 3.2.6, so every Joomla 3 build has been in scope

the whole time. Rather than issue a new number for the Joomla 3 branch, the Joomla CNA is extending that same record, since it is one defect across two branches.

That override was still present, word for word, in the files the 1.0.2 patch shipped for the contact form and the form builder. The opt-in form, the third addon of the same family, was not in the patch at all, so a Joomla 3 site kept whatever it already had there. The one fix in the round that an anonymous attacker could reach without any account was the one the Joomla 3 patch did not apply.

We proved it the same way as on the modern branch: two submissions to the contact addon with the same invalid reCAPTCHA token, identical apart from one field. Without `view_type`, the response was "Invalid Recaptcha". With `view_type=module` and a matching module id, the response was the mail stage, so the captcha gate had already been passed. One field, two outcomes, the same junk token.

Version 1.0.3 removes the module override from all three addons, the opt-in form now included, so the captcha plugin's verdict is the one that counts in every render context.

An XSS fix that stopped one character short

The 1.0.2 patch also introduced a new file, the dynamic content filter addon, as its cross-site scripting fix, and added fifteen `htmlspecialchars` calls to it. Two sinks were missed, and they were on lines the patch itself had edited.

The addon renders a range slider whose minimum and maximum come from a request parameter. On the label line, the value was escaped inside the `data-value` attribute and then printed again, unescaped, as the element's own text content a few characters later:

```
$output .= '<span class="slider-min-value" data-value="'.htmlspecialchars
```

The first `$minValue` is safe. The second, in the text node, was not, so a crafted value reflected straight into the page. The escaping had reached the attribute and stopped before the text a few characters to its right. Version 1.0.3 wraps both, matching the

complete fix already present on the 6.x branch. The Joomla security team assigned it CVE-2026-102426.

The through-line across this vendor's last several rounds is exactly this shape: the fix reaches the reported location and not the sibling running the same code. The 6.8.0 remote code execution sat in the method directly below the one hardened in 6.7.1. Here the correction reached one of two values on a single line, and skipped the opt-in form entirely.

Only 5.6.1 sites can install it

The harder limitation is unchanged from 1.0.2, and it is not about any one finding. The patch checks the installed version and will not run on anything except SP Page Builder 5.6.1 exactly. Across the Joomla 3 sites we monitor that run SP Page Builder, only about 3% are on 5.6.1. For the other 97%, this patch will not install, and neither will 6.9.1. The largest single group is on SP Page Builder 3.8.x, and it has no official fix at all.

There is a second, quieter problem, and it is one we had already raised with JoomShaper. The patch installs as a Joomla file package: it overwrites files in place and, once applied, the component still reports its own version as before. To any updater, and to any scanner that reads a version number, a patched Joomla 3 site looks identical to one that has never been touched. A security fix you cannot detect is one you cannot manage across more than a handful of sites.

Apply 1.0.3 in one click with mySites.guru

A version number cannot tell a patched Joomla 3 site from an unpatched one, so mySites.guru reads the files instead. The Unpatched JoomShaper Security Holes tool runs on each snapshot of a connected Joomla 3 site and looks inside the installed files for a string that exists only in a given release of JoomShaper's patch. For Helix Ultimate, Helix3 and SP Page Builder it reports whether the extension is installed, whether any patch has been applied, and whether the applied patch is the current release. It now

recognises 1.0.3, so a site still on 1.0.2 shows as needing the update rather than as a green tick it has not earned.

Applying the patch is one click on that site's tool page. When you click it, mySites.guru:

- backs up the files the vendor package is about to overwrite, and stops if the backup fails
- downloads JoomShaper's own 1.0.3 package from our CDN and checks it against a pinned SHA-256, so the site receives the exact file JoomShaper published
- installs it through Joomla's own extension installer, so the vendor's version check runs and a site on the wrong SP Page Builder version is turned away, just as it would be if you installed the package by hand
- reports the outcome per extension, so a failed backup, download or install shows up as a failure on the page instead of a success with nothing changed

Undoing it is one click too, restoring the backed-up originals. We install the whole vendor package because the patched files call methods that exist only in other patched files, so splicing them in one at a time would leave a site that fatals.

The tool also covers one hole that no JoomShaper package reaches: a local file include in the SP Page Builder 3.8.x addon loader. The vendor patch installs only onto 5.6.1, so for 3.8.x sites the tool applies a small guard to that one line, with its own backup and its own revert.

Why a monitoring service suits this kind of patch

Joomla's updater, the Extensions manager and any scanner that compares version numbers all read a patched site and an unpatched one as the same, so confirming the fix means opening the files on each site. JoomShaper has also shipped four releases of the SP Page Builder package since July, and several of the Helix Ultimate one, and each new release turns a "patched" site back into an outdated one. mySites.guru repeats the file check on every snapshot of every connected site and flags the ones that fall behind, so you are not keeping a spreadsheet of which client site took which release.

We also read these packages closely ourselves. The two gaps that 1.0.3 fixes were found by us while checking 1.0.2, and the tool moved to 1.0.3 only after we had read the files JoomShaper released.

If you look after Joomla 3 sites that run SP Page Builder, Helix Ultimate or Helix3, [connect them to mySites.guru](#) and the tool will show you which ones are exposed, then patch them in a click. See [pricing](#) for plans.

Apart from that one guard, none of this helps the sites the vendor patch will not install onto. Joomla 3 reached end of life in August 2023, and [the extensions built for it are following it out](#). The fix for those sites is [the migration that has been waiting](#), not another patch. Until then, the findings that need a logged-in account are the ones to think hardest about: audit who holds Author and Editor, and turn off self-registration where nothing depends on it.

Timeline

14 September
2026



SP Page Builder 6.9.1 ships, with a separate Joomla 3 patch

JoomShaper released 6.9.1 for the modern branch and, alongside it, the Joomla 3 Security Patch version 1.0.2 for sites that cannot run 6.x. The Joomla CNA published six CVE records for the 6.9.1 findings the same day, all crediting Phil Taylor of mySites.guru.

14 September
2026



We report two problems in the 1.0.2 Joomla 3 patch

Verifying the released packages, we found the module-context captcha bypass ([CVE-2026-79701](#)) was still live in the files the Joomla 3 patch shipped, with the opt-in form addon not shipped at all, and the patch's cross-site scripting fix escaped only one of the two sinks on the lines it edited. Both proved live on a Joomla 3.10.12 test site, reported to JoomShaper with the Joomla security team copied in.

15 September
2026



JoomShaper acknowledges and starts work

30 September
2026

Support confirmed the report and said the development team would update the Joomla 3 patch.

● **Version 1.0.3 ships, and we verify it**

JoomShaper released the corrected Joomla 3 Security Patch, version 1.0.3. We read the released files and confirmed the module-context captcha shortcut is gone from all three form addons, the opt-in form is now shipped, both dynamic content filter sinks are escaped, and the captcha type is read from the stored addon rather than the request.

30 September
2026

● **The Joomla CNA assigns the CVE numbers**

The Joomla security team assigned CVE-2026-102426 for the dynamic content filter XSS, and extended the existing [CVE-2026-79701](#) to cover the Joomla 3 branch for the captcha bypass rather than issuing a new number, since it is the same defect on an older branch.

Further Reading

- [The SP Page Builder 6.9.1 disclosure](#) - the full round this Joomla 3 patch back-ports, including the SQL injection and the captcha bypass mechanism in detail.
- [JoomShaper's Joomla 3 Security Patch for SP Page Builder](#) - the vendor's download page for the patch package.
- [JoomShaper's third Joomla 3 security patch for Helix Ultimate](#) - the same file-package pattern, and the same version-invisibility problem, in a sibling product.
- [CWE-79: Cross-site Scripting](#) and [CWE-807: Reliance on Untrusted Inputs in a Security Decision](#) - the weakness classes behind the two issues.
- [JoomShaper](#) - the vendor's site.
- [JoomShaper's Joomla 3 record](#) - what JoomShaper has said and shipped for Joomla 3, in date order, with sources.

Frequently Asked Questions

What changed in the SP Page Builder Joomla 3 Security Patch 1.0.3?

It finishes the job the earlier 1.0.2 patch started. Version 1.0.2 back-ported four of the five SP Page Builder 6.9.1 fixes to the Joomla 3 branch but left the captcha bypass live and shipped an incomplete cross-site scripting fix. Version 1.0.3 removes the module-context captcha shortcut from all three form addons, including the opt-in form that 1.0.2 never shipped, escapes both halves of the dynamic content filter output, and reads the captcha type from the stored addon rather than the request. We reported both gaps on 14 September 2026 and confirmed 1.0.3 closes them.

Was the captcha bypass really still live on Joomla 3?

Yes. The module-context captcha bypass, published as [CVE-2026-79701](#), was fixed on the modern 6.x branch in SP Page Builder 6.9.1, but the code that discards the real captcha result whenever the request claims the form sits inside a module was still present in the files the 1.0.2 patch shipped. We proved it on a Joomla 3.10.12 test site with the patch files in place: two form submissions with the same invalid reCAPTCHA token, identical except for one field, one rejected and one accepted. The published affected range for [CVE-2026-79701](#) already reaches back to 3.2.6, so every Joomla 3 build was in scope from the start. The 1.0.2 patch simply did not apply the fix there. 1.0.3 does.

Which Joomla 3 sites can install version 1.0.3?

Only sites running SP Page Builder 5.6.1 exactly. The patch checks the installed version and will not install on anything else, which is the same limit 1.0.2 had. Across the Joomla 3 sites we monitor that run SP Page Builder, only about 3% are on 5.6.1. The rest cannot install this patch and cannot install 6.9.1 either, so their only real fix is migrating off Joomla 3.

Is there a CVE for the cross-site scripting issue?

Yes. The Joomla security team assigned CVE-2026-102426 for it. The reflected XSS lived in the dynamic content filter addon's range-slider labels: the 1.0.2 patch escaped the attacker-controlled value inside the data-value attribute but echoed the same value unescaped as the element's text a few characters later. The captcha bypass is not getting a second number, because the Joomla CNA is extending the existing [CVE-2026-79701](#) to cover the Joomla 3 branch, since it is the same defect on an older branch.

Can mySites.guru apply the SP Page Builder Joomla 3 patch for me?

Yes. The Unpatched JoomShaper Security Holes tool in mySites.guru checks every connected Joomla 3 site for SP Page Builder, Helix Ultimate and Helix3, reads the installed files to see which JoomShaper patch release is in place, and applies the current one in one click. It backs up the files first, verifies JoomShaper's package against a pinned SHA-256, installs it through Joomla's own installer, and can revert it in one click. Sites still on 1.0.2 show as needing the 1.0.3 update.

What do I do if my Joomla 3 site cannot install the patch?

Plan the migration. Joomla 3 reached end of life in August 2023 and the extensions built for it are being retired alongside it. The vendor's patch installs onto SP Page Builder 5.6.1 and nothing else, so the large group of sites on 3.8.x and other older builds get no official fix at all. In the meantime, tighten what an attacker can reach without one: audit who holds Author and Editor, and turn off self-registration if nothing depends on it. mySites.guru flags every connected site still running an affected build so the list is in front of you rather than site by site.

AI MODIFIED

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

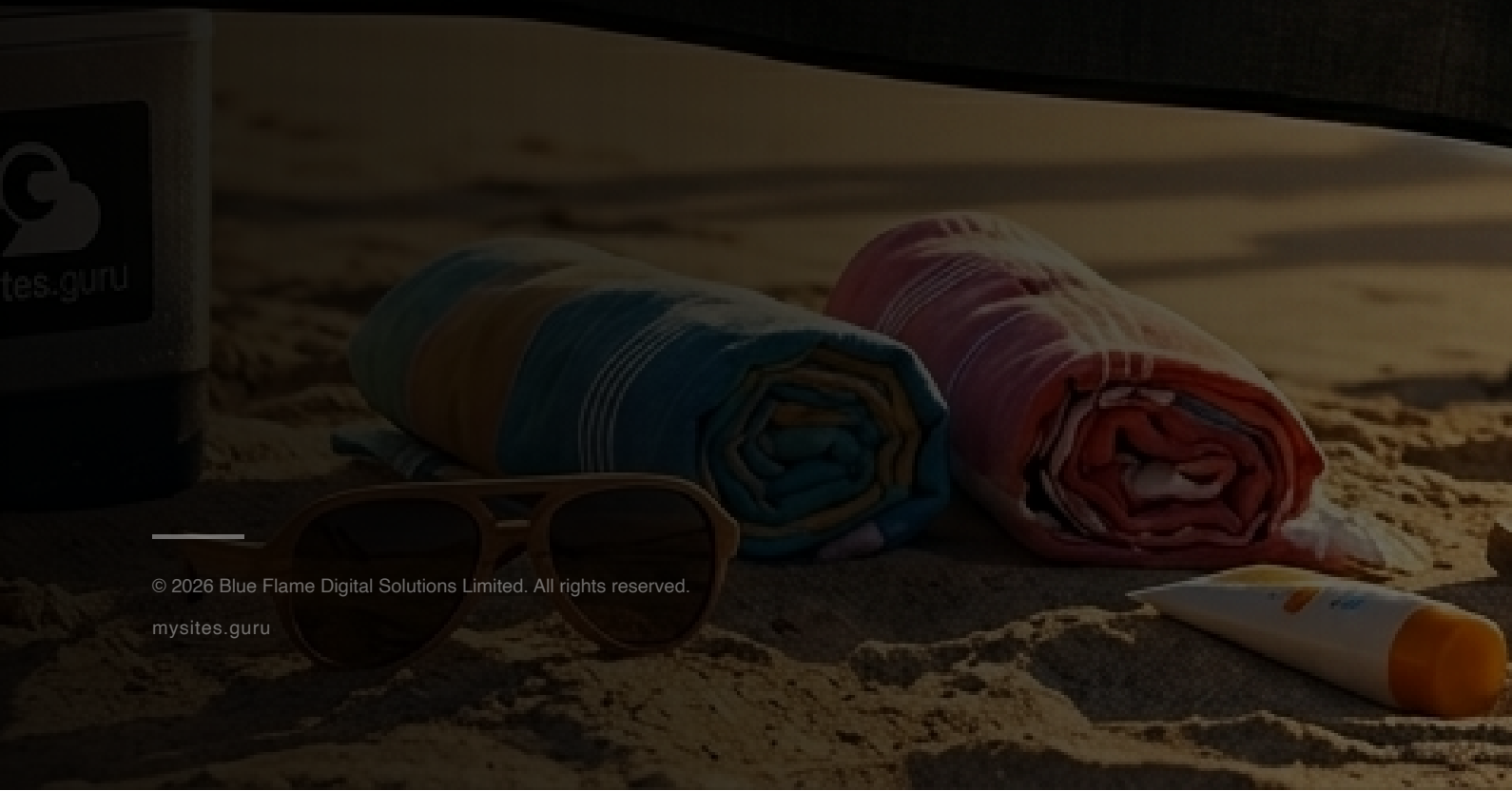
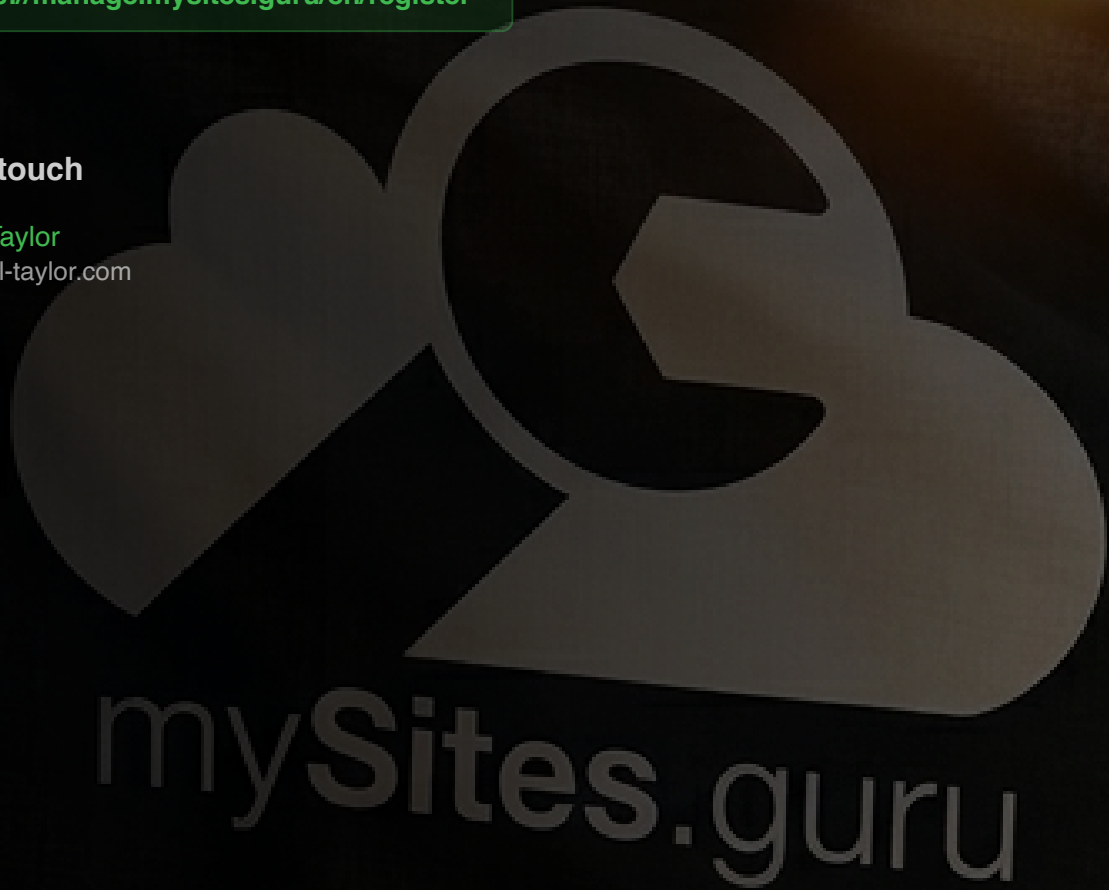
Get Your Free Site Audit

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