



Quix Page Builder 6.3.4 Fixes Guest Access and Editor Code Execution Flaws

Quix Page Builder 6.3.4 stops guests changing Quix settings or reading restricted pages, and editors running code on the server. Update every Joomla site.

Phil E. Taylor | 30 September 2026

ThemeXpert released [Quix Page Builder 6.3.4](#) on 30 September 2026, and its changelog has a Security section with three entries. A visitor who was not logged in could change Quix settings and read pages restricted by access level. An editor could run code on the server. Text taken from Joomla articles could run scripts on Quix pages. Quix is a Joomla extension, not part of Joomla itself, so this affects only sites that have Quix installed.

This is the fifth Quix security release since the middle of July, and the numbers from the Quix sites mySites.guru monitors say that most of them have not installed any of the other four. If you run Quix anywhere, update to 6.3.4, and read on for why the sites furthest behind need more than one update.

TL;DR

- **Quix 6.3.4** fixes guest access to Quix settings and restricted pages, code execution by editors, and script injection from Joomla article text. It also hardens pasted images, image resizing and the bundled JMedia media manager
- ThemeXpert gives **no affected range, no severity and no CVE**. Treat every version below 6.3.4 as affected
- It is the **fifth Quix security release in eleven weeks**, after 6.2.1, 6.2.2, 6.2.4 and 6.2.7
- Across the Quix sites mySites.guru monitors, **more than half are still below 6.2.2**, so they also miss the July fix for an unauthenticated SQL injection
- mySites.guru flags every connected Joomla site below 6.3.4 from the day of the release

What the Quix 6.3.4 changelog says

The release notes on GitHub and the [changelog.xml](#) that Joomla's update screen links to have the same three security entries, word for word:

- "Pages: editors can no longer run code on the server, and guests can no longer change Quix settings or read access-restricted pages."
- "Joomla Content: text from articles, including titles and categories, can no longer run scripts on Quix pages."
- "Media: pasted images, image resizing and the bundled JMedia media manager are hardened."

The rest of the release is ordinary maintenance: forms displaying on Joomla 4 again, builder errors when JCE is the default editor, and icons now stored on your own site instead of being fetched from getquix.net. One version ships for Joomla 3.10, 4, 5 and 6, so there is no second release line to track.

Read from the changelog, not the code

ThemeXpert's public GitHub repository holds release notes and update metadata, not source code, and we have not diffed the 6.3.4 package. What follows reads the vendor's wording for what it means on a site. We have not reproduced the flaws.

What each Quix 6.3.4 fix means for a Joomla site

Guests could change Quix settings and read restricted pages

In Joomla terms a guest is anyone who is not logged in, so this is the entry that matters most: it needed no account. Changing Quix settings from outside is an integrity problem with no obvious ceiling, because the settings decide how Quix loads and renders every page it builds. Reading "access-restricted pages" means a Quix page set to Registered, or to a custom access level for members or clients, could be read by an anonymous visitor.

If you use Joomla access levels to keep Quix pages private (a client area, a members' price list, a staff page) assume their contents could have been read until the site was updated.

Editors could run code on the server

The changelog does not say which editors, but in a page builder that means an account allowed to build or edit Quix pages, which on most agency sites is more people than just the Super Users. Code execution on the server is the most serious class of flaw a Joomla extension can have, and editor accounts are the ones that get phished or reused.

It is also the second time. The [6.2.1 changelog](#) in July fixed "a code-execution path via the Raw HTML element", one of the issues [we reported to ThemeXpert](#) and tracked as [CVE-2026-60026](#). Whether 6.3.4 closes a different path or a gap in that fix, ThemeXpert does not say.

A malicious actor's own code runs on your server, with the same access as the website itself: reading, changing or deleting any file it can touch, planting a backdoor that survives the next update, installing malware, pulling every database credential and API key from your configuration, and using your server to attack other people. Gulp.

Joomla article text could run scripts on Quix pages

Quix has elements that pull in Joomla articles, and the changelog says their titles, categories and text reached the Quix page without being escaped. That makes it stored cross-site scripting: whoever can write an article, including a front-end author on a site that allows one, could place a script that runs for every visitor to the Quix page showing that article, and for any administrator who views it while logged in.

Media handling was hardened

"Hardened" is vendor language for something that was not safe enough, with no detail given. It covers pasted images, image resizing and JMedia, the media manager Quix bundles. JMedia had three flaws of its own fixed in July, including a file upload that led

to code execution ([CVE-2026-60032](#)), so this is another area that has needed work more than once.

Five Quix security releases in eleven weeks

ThemeXpert's own changelog puts a Security section on five releases since mid-July. Quix 6.2.0, released just before our July report, described itself as a completed full security audit.

Release	Date	What the Security section fixed
6.2.1	15 July 2026	Unauthenticated SQL injection, Raw HTML code execution, form path traversal, icon XSS, media manager permission, JMedia upload and SSRF
6.2.2	16 July 2026	The unsanitised CSS ID and Class fields
6.2.4	26 July 2026	Unauthenticated page creation with a bare CSRF token, missing permission checks on collections, a guessable login cookie
6.2.7	18 August 2026	SQL injection in the Joomla Articles element, unauthorised session and cookie changes, bundled libraries
6.3.4	30 September 2026	Guest access to settings and restricted pages, editor code execution, article text XSS, media

ThemeXpert writes clearer changelogs than most Joomla vendors and names the flaw class in plain words. Read together, though, several of these releases fix the same kind of mistake: who is allowed to do what. Unauthenticated page creation in 6.2.4, unauthorised session changes in 6.2.7 and guest settings changes in 6.3.4 are all permission checks that were missing. A page builder exposes a lot of AJAX endpoints to the front end, and each one is a place to forget a permission check.

How far behind are Quix sites?

Among the Joomla sites in the mySites.guru database that run Quix and took a snapshot in the 30 days to 30 September 2026:

Installed Quix version	Share of sites
Below 6.2.2	52%
6.2.2 to 6.2.6	9%
6.2.7 to 6.3.3	39%

More than half have not installed 6.2.2, which means they still have the unauthenticated SQL injection we reported in July, which lets an anonymous visitor read the site's database. About half of all Quix sites run Quix 5 or older, and Quix 2.x alone accounts for a third of all Quix sites. All the Security sections in ThemeXpert's changelog belong to Quix 6 releases, so those sites have to get onto Quix 6 before 6.3.4 means anything to them. Try that on a copy of the site first: a jump of several major versions is not a routine update.

The 39% on 6.2.7 or later are the easy case: one update to 6.3.4 and they are current. The other 61% need 6.3.4 for this release and pick up the July and August fixes in the same step.

Which of your sites need Quix 6.3.4?

mySites.guru records the installed version of every extension on every connected Joomla site twice a day. The Quix rule for versions below 6.3.4 went live on the day of the release, so affected sites are flagged on their dashboards and in their audits, and the [Quix page of our vulnerability list](#) shows it alongside the two earlier Quix rules. A site below 6.2.7 is flagged by the older Quix rules instead, whose warnings describe the earlier flaws, and updating it to 6.3.4 clears all of them.

From there, [update the flagged sites from one dashboard](#) rather than logging into each administrator in turn, or let [automatic extension updates](#) install Quix releases as they come out, which with five security releases in eleven weeks is the setting that would

have kept a site current without anyone watching. The [vulnerable extension list](#) puts Quix alongside the other flagged extensions on your sites.

What to check after updating Quix

Updating closes the holes. It does not remove anything that got in first. On a site that ran an affected version, work through these:

1. List the accounts that can build or edit Quix pages and remove any you do not recognise. An unfamiliar Super User is the clearest sign of a successful code execution.
2. Open Quix's global options and check them against what you set, because guests could change them.
3. Look at the compiled page files. In the Quix code we audited in July, pages are compiled to PHP files under `media/quixnxt/storage/`. A file there that does not belong to one of your pages, or that contains more than template output, needs a closer look.
4. On a site with front-end authors, check recently edited articles that appear on Quix pages for `<script>` tags or event handlers in the title or text.

Find Super User accounts you did not create

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

The same audit checks for [hacked files and backdoors](#) and PHP files in folders that should only hold media, and [real-time alerting](#) tells you when a file changes or an

unfamiliar administrator logs in. If you find something you did not put there, treat the site as compromised: [our Joomla hacked-site guide](#) sets out the order of work, and [fix.mySites.guru](#) will clean it up for a single fixed fee.

What we would like from ThemeXpert

A CVE with an affected range and a severity would let other scanners flag these sites too. Earlier Quix fixes got their CVEs from the Joomla CNA days after release, so these may follow, and we will add them to the rule when they do. Until then, the changelog is all anyone has, and the only safe reading of it is "all versions below 6.3.4".

If you look after more than a handful of Joomla sites, the Quix history since July is the argument for checking installed versions continuously rather than when a vendor sends an email. [See what mySites.guru costs](#) for the number of sites you manage.

Further Reading

- [Quix 6.3.4 release on GitHub](#) - ThemeXpert's release notes, published 30 September 2026
- [Quix changelog.xml](#) - the full Quix release history, with a Security section on each release from 6.2.0 on
- [Quix Page Builder on the Joomla Extensions Directory](#) - the listing, reviews and supported Joomla versions
- [Unauthenticated SQL Injection in Quix Page Builder](#) - the seven issues we reported in July, fixed in 6.2.1 and 6.2.2

Frequently Asked Questions

Is Quix Page Builder 6.3.4 a security release?

Yes. Its changelog has a Security section with three entries: editors can no longer run code on the server, guests can no longer change Quix settings or read access-restricted pages, and text from Joomla articles can no longer run scripts on Quix pages. Pasted images, image resizing and the bundled JMedia media manager were hardened as well.

Which Quix versions are affected by the 6.3.4 fixes?

ThemeXpert does not say which version introduced each flaw, only that 6.3.4 fixes them. Treat every Quix version below 6.3.4 as affected. Sites below 6.2.7 also miss the fixes from ThemeXpert's earlier security releases, so they are exposed to more than this one.

Do the Quix 6.3.4 flaws have CVE numbers?

Not at the time of writing. ThemeXpert published the fixes in its changelog on 30 September 2026 with no advisory and no CVE. Earlier Quix fixes were given CVEs by the Joomla CNA some days after release, so ids may follow.

Can an anonymous visitor exploit Quix below 6.3.4?

Some of it, yes. The changelog says guests could change Quix settings and read pages restricted by access level, and a guest is a visitor who is not logged in. The code execution needs an account with editor access to Quix, and the script injection needs someone able to write article text.

Is Quix 6.3.4 the free or the Pro version?

The release notes are for the free edition, published on GitHub. Quix Pro uses the same version numbers as the free edition, so update whichever you run to 6.3.4, and if your Pro download does not offer 6.3.4 yet, ask ThemeXpert when it will.

Does mySites.guru flag Quix below 6.3.4?

Yes. The rule went live on the day of the release, so every connected Joomla site running an affected Quix version is flagged on its dashboard and in its audit, alongside the earlier Quix rules.

AI MODIFIED

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

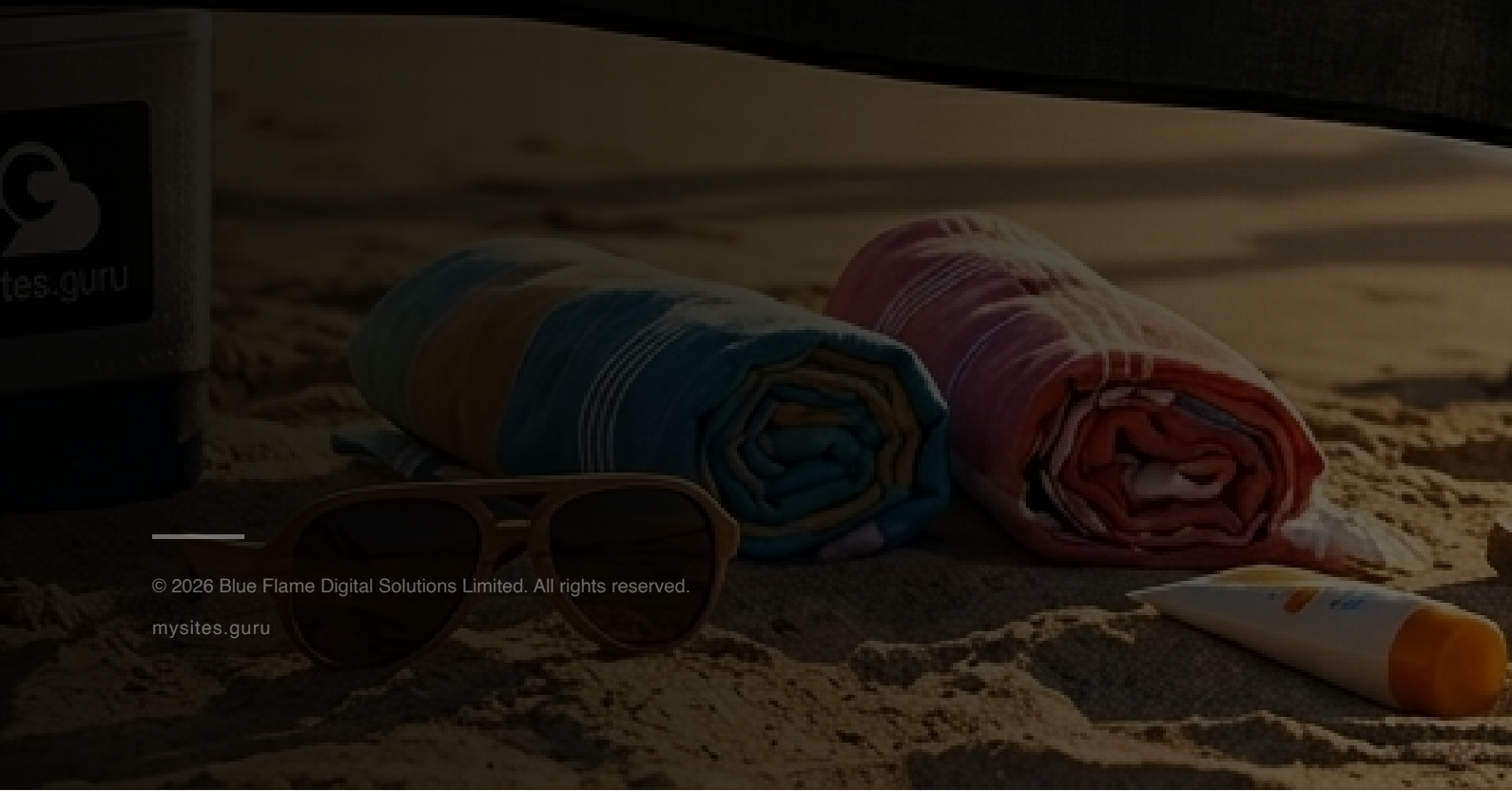
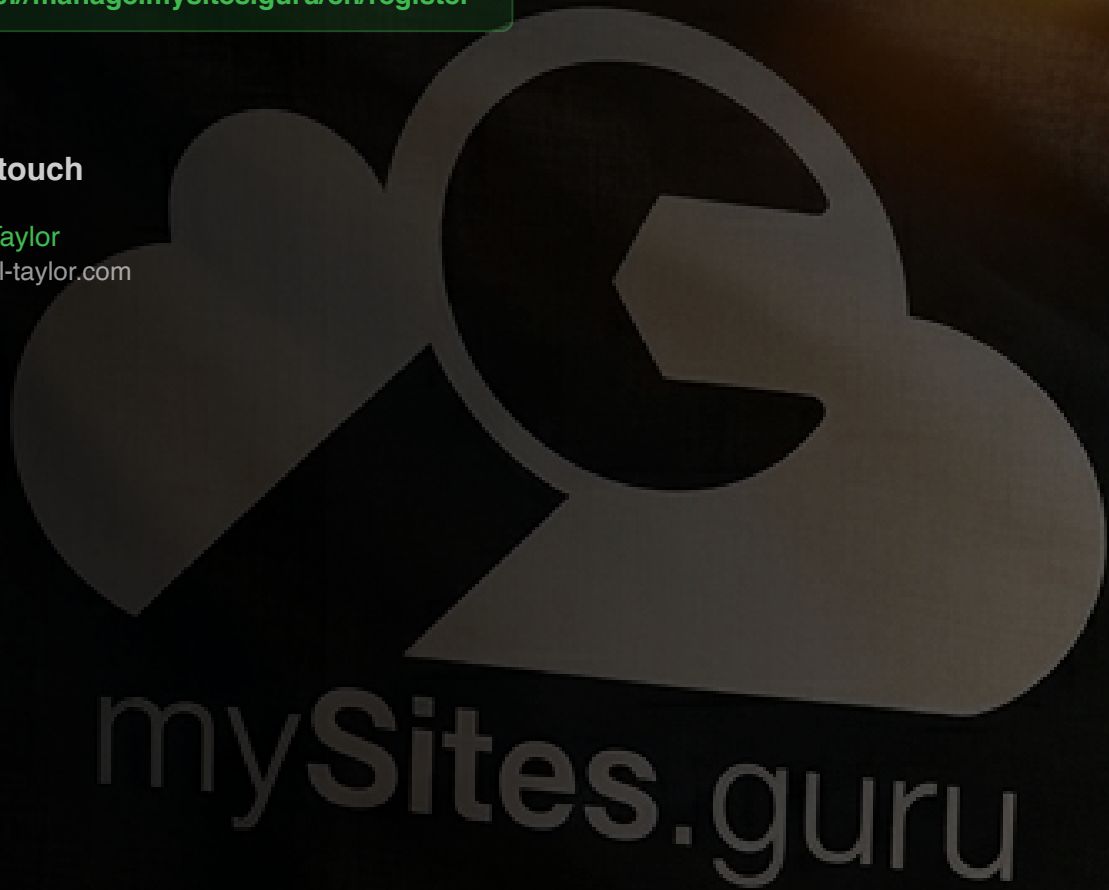
Get Your Free Site Audit

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