



Quix Page Builder 6.4.0 Stops Guests Reading Access-Restricted Joomla Articles

Quix Page Builder 6.4.0 fixes an AJAX handler that let anyone read Joomla articles restricted to Registered or custom access levels. Update every Joomla site.

Phil E. Taylor | 27 October 2026

ThemeXpert released Quix Page Builder 6.4.0 on 27 October 2026 with a single entry in its Security section: the Joomla Article and Joomla Articles elements now respect article access levels, so visitors only see articles they are allowed to read. Quix is a Joomla extension, not part of Joomla itself, so this concerns only sites that have Quix installed.

That one line understates it. We diffed the 6.3.6 and 6.4.0 packages, and the code shows that before this release a visitor who was not logged in could fetch the full text of any published Joomla article on the site by its id, including articles set to Registered, Special or a custom access level, whether or not the article had ever been placed on a Quix page.

TL;DR

- **Quix 6.4.0** fixes a front-end AJAX handler that returned any published Joomla article to anyone, ignoring the article's access level
- The flaw is read-only and needs no account. What it exposes is whatever a site keeps in restricted articles: members' content, client areas, staff notes, paid content, price lists
- ThemeXpert gives **no affected range, no severity and no CVE**. Treat every Quix version below 6.4.0 as affected. Our own assessment is 6.9, Medium
- It is the sixth Quix release since mid-July with a real security fix, and the fourth to fix a missing permission check
- After updating, clear Quix's cache and Joomla's cache: a page rendered for a member before the update can still be sitting in the cache
- mySites.guru flags every connected Joomla site below 6.4.0 from the day of the release

6.9

CVSS 4.0

Quix 6.4.0: unauthenticated read of access-restricted articles (no CVE yet)

MEDIUM

mySites.guru (our assessment, no CVE or vendor score yet)

An anonymous visitor can read the full text of any published Joomla article by id, whatever access level it is set to, but cannot change data or run code.

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

No login needed

Read only

Joomla Article element

▼ 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:L Low: Some data can be read

VI:N None: Nothing 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

What the Quix 6.4.0 changelog says

The release notes on GitHub and the [changelog.xml](#) that Joomla's update screen reads have one security entry, word for word:

- "Joomla Article and Joomla Articles elements now respect article access levels, so visitors only see articles they are allowed to read."

There is no advisory, no severity, no affected range and no reporter named.

ThemeXpert found and fixed this one itself. Everything below about how it worked comes from comparing the 6.3.6 and 6.4.0 packages.

The rest of 6.4.0 is a normal feature release: new Atom template layouts for Joomla 4, 5 and 6, updating now refreshes already-published pages, faster pages, Joomla 5 and 6 no longer need the Behaviour - Backward Compatibility plugin, and several Joomla 6 error-page fixes. One release line covers Joomla 3.10 to 6, so there is no second version to track.

What the Quix code change shows

The Joomla Article element places one Joomla article on a Quix page. To fetch that article it has a front-end AJAX handler that anyone can call without logging in, and the handler takes the article id from the request. That shape, a public endpoint that does a job on behalf of whoever calls it, is the one we described in [AJAX endpoints as a CMS security blind spot](#).

In 6.3.6 the handler told Joomla's article model that access had already been checked. It set the model's access filter whenever com_content's "show unauthorised links" option (show_noauth) was off, which is the default on a Joomla site. Joomla's model then treats the article as viewable by everyone and returns it in full. The handler skipped the check of whether this visitor may read this article, so any published article could be read by id.

6.4.0 removes that shortcut and leaves the model to work out access for the current visitor. Without access it returns nothing, or only the intro text where show_noauth is on, which matches what Joomla's own article view does.

The Joomla Articles element, which lists articles, had a smaller version of the same problem. Where show_noauth is on, the list includes articles the visitor cannot read,

and its AJAX response sent each whole item, full text included. 6.4.0 blanks the full text for those.

The last part of the change concerns caching. Quix caches each rendered page once for all visitors. In 6.3.6 a page that showed a restricted article to a logged-in member could be cached and then served to the next visitor, who was not logged in. 6.4.0 keeps such renders out of Quix's cache and out of Joomla's page cache. It does this through a new helper class, `ArticleAccess`, whose own code comment notes that element helpers answer both the public AJAX route and the page render, which is a fair summary of why the AJAX route needed the same check as the page.

Which Joomla sites lose something from the Quix flaw

The impact is confidentiality only. The flaw reads article text; it does not change anything, does not run code and needs no account. That is why our CVSS 4.0 score is 6.9, Medium, with confidentiality marked Low: it exposes article text rather than the whole database.

Whether that matters on your site depends on one thing: do you use Joomla access levels to keep any articles private? A site whose articles are all Public has nothing to lose from this flaw, because anyone could already read them. A site that keeps members' content, a client area, staff notes, paid content or a price list in Registered, Special or custom-level articles should assume those articles could have been read by anyone until the site was updated. Both kinds of site still need 6.4.0, because a site below 6.3.4 also misses the [earlier Quix security releases](#).

The same Quix mistake, again

Quix 6.3.4, four weeks ago, fixed guests reading access-restricted Quix pages. Quix 6.4.0 fixes guests reading access-restricted Joomla articles shown through Quix elements. It is the same class of mistake, moved one layer down.

Counting only releases with a real security fix, 6.4.0 is the sixth since mid-July: 6.2.1 on 15 July, 6.2.2 on 16 July, 6.2.4 on 26 July, 6.2.7 on 18 August, 6.3.4 on 30 September and now 6.4.0. (6.3.6 on 14 October had a Security section too, but its only note was that public pages no longer load the axios library, so scanners stop reporting its CVEs. That is a tidy-up, not a fix.) Four of the six fixed a missing permission check: unauthenticated page creation in 6.2.4, unauthorised session changes in 6.2.7, guest settings changes and restricted pages in 6.3.4, and restricted articles in 6.4.0.

This one is an authorisation failure in its simplest form, the difference between authentication and authorisation in one handler: Joomla knew whether the visitor was logged in, and the handler never asked whether that visitor could read the article they named. ThemeXpert writes clearer changelogs than most Joomla vendors, and it keeps fixing the problems it finds. A page builder exposes a lot of front-end endpoints, and each one is a separate place to forget that question.

Quix sites four weeks after 6.3.4

Among the Joomla sites in the mySites.guru database that run Quix and took a snapshot in the 30 days to 27 October 2026:

40%

on 6.3.4 to 6.3.6

Affected by this flaw only; one update to 6.4.0 makes them current

3%

on 6.2.7 to 6.3.3

Down from 39% on 30 September

51%

still below 6.2.2

52% on 30 September; still open to the July SQL injection. Nearly all run Quix 5 or older

Joomla sites running Quix with a snapshot in the 30 days to 27 October 2026, mySites.guru database. Percentages of those sites.

On 30 September, 39% of these sites were on 6.2.7 to 6.3.3 and none had 6.3.4 yet. Four weeks later only 3% remain in that band and 40% are on 6.3.4 or later. Nearly every site that was keeping up with Quix installed the September release within a month, which is a good result for any Joomla extension.

The other half of the chart did not move. 52% were below 6.2.2 in September, 51% are below it now, and they still have the [unauthenticated SQL injection we reported in July](#). Our reading of the two snapshots is that a security release helps the sites that are already updating. The sites that most need one do not see it, because no one is checking the version they run.

Which of your Joomla sites need Quix 6.4.0?

mySites.guru records the installed version of every extension on every connected Joomla site twice a day. A rule for Quix 6.3.4 to 6.3.6 went live on the day of the release, and the earlier Quix rules cover every older version, so every connected Joomla site below 6.4.0 is flagged on its dashboard and in its audit. The [Quix page of our vulnerability list](#) shows all of them together.

From there, [update the flagged sites from one dashboard](#) rather than logging into each administrator in turn, or switch on [automatic extension updates](#) so the next Quix release installs itself. With six security fixes since July, that setting keeps a site current without anyone watching. The [vulnerable extension list](#) puts Quix alongside every other flagged extension on your sites.

What to do after updating Quix

1. Update Quix to 6.4.0, free or Pro. Quix Pro uses the same version numbers as the free edition. If your Pro download does not offer 6.4.0 yet, ask ThemeXpert.
2. Clear Quix's cache and Joomla's cache. 6.4.0 keeps restricted renders out of both caches from now on, but a page cached before the update, possibly with a member's view of a restricted article in it, stays until it is rebuilt.

3. Review what you keep in restricted articles. Anything in a Registered, Special or custom-level article should be treated as possibly read by anyone up to the moment of the update.
4. Change anything secret that was kept in an article: passwords, access codes, links to private files. A private link stops being private once someone else has read it.

We know of no workaround short of updating.

If you look after more than a handful of Joomla sites, the two Quix snapshots above make the case for checking installed versions continuously instead of waiting for a vendor email. [See what mySites.guru costs](#) for the number of sites you manage.

Further Reading

- [Quix 6.4.0 release on GitHub](#) - ThemeXpert's release notes, published 27 October 2026
- [Quix changelog.xml](#) - the full Quix release history, with a Security section on each release that fixed one
- [Quix Page Builder on the Joomla Extensions Directory](#) - the listing, reviews and supported Joomla versions
- [Quix 6.3.4 Fixes Guest Access and Editor Code Execution Flaws](#) - the previous Quix security release, four weeks earlier
- [AJAX Endpoints Are A Big CMS Security Blind Spot](#) - why front-end AJAX handlers keep missing permission checks
- [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 6.4.0 a security release?

Yes. Its changelog has one Security entry: the Joomla Article and Joomla Articles elements now respect article access levels. Before 6.4.0, a visitor who was not logged in could fetch the full text of any published Joomla article by id through a Quix AJAX handler, including articles restricted to Registered, Special or a custom access level.

Which Quix versions are affected?

ThemeXpert does not say when the flaw started. The 6.3.6 code has the same access line, so treat every Quix version below 6.4.0 as affected. Sites below 6.3.4 also miss the earlier Quix security releases.

Does the Quix 6.4.0 flaw have a CVE?

Not at the time of writing. ThemeXpert published no advisory, no severity and no reporter. Our own CVSS 4.0 assessment is 6.9, Medium, because an anonymous visitor can read article text but cannot change anything or run code.

Which Joomla sites actually lose something from this flaw?

Sites that use Joomla access levels to keep articles private: members' content, client areas, staff notes, paid content or price lists. A site whose articles are all Public has nothing to lose from this flaw but still needs 6.4.0 for the rest of the Quix security history.

Why clear the cache after updating Quix to 6.4.0?

Quix caches each rendered page once for all visitors, and in 6.3.6 a page rendered for a logged-in member could be cached and served to the next anonymous visitor. 6.4.0 keeps such renders out of the cache, but a page cached before the update is still there until you clear Quix's cache and Joomla's cache.

Does mySites.guru flag Quix below 6.4.0?

Yes. A rule for Quix 6.3.4 to 6.3.6 went live on the day of the release, and earlier rules cover older versions, so every connected Joomla site below 6.4.0 is flagged on its dashboard and in its audit.

AI MODIFIED

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

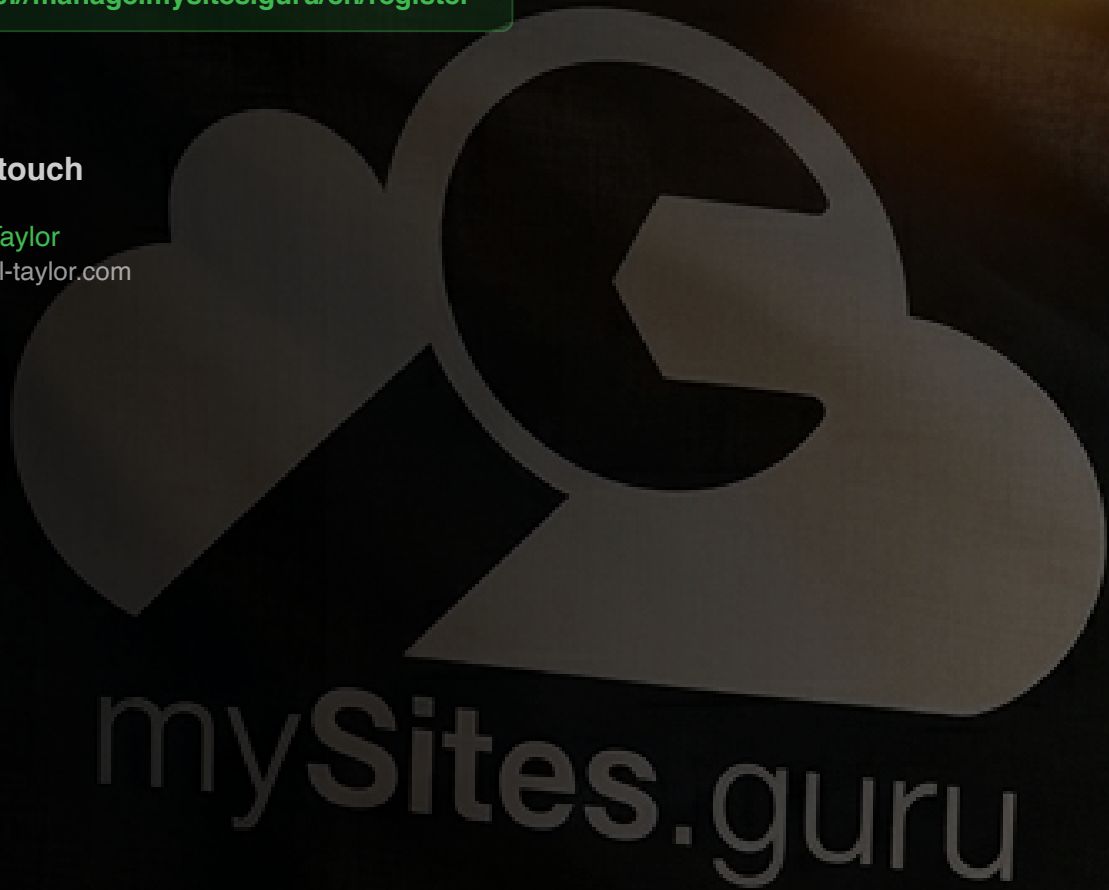
Get Your Free Site Audit

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