



# JCH Optimize 9.4.0 Fixes Six High-Rated Security Issues in the Joomla Extension

JCH Optimize 9.4.0 fixes an XSS, an unauthenticated hit counter flaw, missing admin CSRF checks and an open redirect. What changed, who is exposed, how to fix.

Phil E. Taylor | 7 October 2026

JCH Optimize is a page speed extension for Joomla: it combines and minifies CSS and JavaScript, rewrites HTML, optimises images and serves a page cache. This morning its developer, Samuel Marshall, released JCH Optimize 9.4.0 and called it "a security and maintenance release". The changelog rates six of the fixes HIGH, including a cross-site scripting issue, an unauthenticated Page Cache endpoint and administrator tasks that ran without a security token.

Every version before 9.4.0 is affected, in both the Free and Pro editions. No CVE has been published and the release credits no finder. If a Joomla site you manage runs JCH Optimize, update it to 9.4.0 today.

## Update, 7 October 2026: Pro sites using the Redis cache

A JCH Optimize Pro user reported this afternoon that 9.4.0 takes down sites that use Redis as the cache store, with a fatal "Redis\Metadata is not available" error on every page. We confirmed it in the 9.4.0 Pro package. 9.4.0 upgrades its bundled Laminas Redis adapter from 2.2 to 3.1.0, whose `Redis` class depends on a `Redis\Metadata` class in a `src/Redis/` folder. The Pro package ships none of the four files in that folder, `Metadata.php` included, and its class map does not list them. The Free edition has no Redis adapter at all, so it is not affected, and Pro sites using the default Filesystem storage are not affected either.

If a Pro site uses Redis, set JCH Optimize's Storage Adapter (in the Cache Storage settings) to Filesystem before you update, and switch it back once the vendor ships a fixed build. The setting's own fallback to Filesystem does not help here, because a missing class stops PHP before JCH Optimize can catch it. If a site is already down, renaming the `plugins/system/jchoptimize` and `plugins/system/jchpagecache` folders over FTP brings the front end back while you sort out the storage setting or restore a backup.

## How mySites.guru flags JCH Optimize below 9.4.0

mySites.guru records the exact version of every extension on every connected Joomla site twice a day. We added JCH Optimize 9.4.0 to our [Joomla vulnerability database](#) the afternoon it was released, so any connected site running the component or its system plugin below 9.4.0 is now flagged on its own site card and in its audit, with the version that resolves it.

The rule matches the component and the system plugin separately. JCH Optimize installs several plugins that share the element name `jchoptimize` (a console plugin and, from 9.4.0, a scheduler task plugin), and those are versioned alongside the main extension, but the rule is pinned to the component and the `system` plugin so that a stray row cannot flag a site that has already updated.

## What the mySites.guru database shows

JCH Optimize is one of the more common third-party extensions we see. These figures are from the Joomla sites connected to mySites.guru that reported in during the last 30 days, taken the afternoon 9.4.0 was released:

**1 in 10**

connected Joomla sites run JCH Optimize

**99%**

of current-line installs were below 9.4.0  
on release day

**1 in 4**

JCH Optimize sites are on the old Joomla  
3 line, which has no fix

The second figure is normal for the first day of any release. The third will not change by itself, because the old line has no patch to wait for.

## The cross-site scripting issue in the JCH Optimize optimiser

The first HIGH item in the changelog is "a cross-site scripting vulnerability where encoded characters in URLs, such as search query links, were decoded during optimization". JCH Optimize rewrites the HTML of every page it serves. Going by the vendor's description, when Joomla or another extension has already escaped a value inside a link, for example a search term echoed into a "search again" URL, the optimiser's rewriting step could turn the encoded characters back into live ones.

The rest of the site did nothing wrong here. Joomla escaped the value correctly; the extension sitting between Joomla and the browser undid it. An attacker only has to get a visitor, or an administrator, to open a crafted search link, and the script runs in the context of the site.

This is the one to worry about first on a busy public site, because it needs no account and it reaches any visitor who follows the link.

## The Page Cache hit counter ran any component's model

When JCH Optimize serves a page from its own page cache, Joomla never runs the component that built the page, so article hit counters would stop moving. To fix that, the Page Cache plugin adds a small script to cached pages that calls back to the site and records the hit.

We compared the 9.3.1 and 9.4.0 Free packages to see what the vendor's description, "allowing a request to run any component's model", means in practice. In 9.3.1 the callback is a `com_ajax` endpoint in `plg_system_jchpagecache` that answers anonymous requests. It reads a component name ( `hitoption` ) and a model name ( `hitview` ) from the request, boots that component, builds the named site model and calls its `hit()` method with an ID from the request. If anything throws, the exception message is sent back in the response.

So any visitor could choose which component and which model to run, and drive hit counters on content the page cache never served, including unpublished items and content behind access levels. We have not shown it reaching anything worse than `hit()`, and the vendor does not say it does. 9.4.0 replaces the endpoint's logic with a fixed list of supported pages (articles, categories, contacts, news feeds and tags) and checks that the item is published and visible to the visitor before counting it.

## Admin tasks ran without a token or the `core.admin` permission

The 9.4.0 changelog says administrator tasks that change settings or files now "require a valid form token and administrator permissions". The diff shows where the check went in. JCH Optimize 9.4.0 adds a guard to its administrator dispatcher: anything other than a read-only dashboard view now needs the `core.admin` permission on the component and a valid Joomla session token.

In 9.3.1 neither check was there, which allowed:

- Cross-site request forgery: a logged-in administrator who opened a crafted link or page could be made to change JCH Optimize settings or run its file tasks without knowing it.
- Weaker permissions than the job needs: a backend user who could open the component, but who should not be configuring it, could change settings that alter every page the site serves.

The same release stops settings exports from including the Cloudflare API token and the Redis password, and keeps a site's existing token and password when an import file leaves them out. An old export file sitting in a downloads folder or a support ticket still holds both.

## Image paths, the open redirect and the `jchbackend` switch

The remaining HIGH items are narrower:

- Image optimisation paths: the image optimisation service returns URLs and file paths for the optimised images. 9.4.0 validates those and keeps image folders inside the site root, where earlier versions trusted what came back.
- Open redirect: the Mode Switcher and Utility tasks redirected to whatever URL was passed, base64 encoded, in the `return` parameter. 9.4.0 only follows a return URL on the site itself. The controllers sit on the administrator side, so the link has to be followed by someone logged in there, which is exactly who a phishing redirect wants.
- The jchbackend parameter: adding `jchbackend=1` to any front-end URL told JCH Optimize to skip optimisation for that request, for any visitor. 9.4.0 removes the parameter.

The MEDIUM items harden the page cache against malformed `Host` headers and unsafe characters in Capture Cache file paths, and escape file and folder names in the Optimize Images file tree. One small fix shows how these things slip through: in 9.3.1 the check for the `jchnooptimize` parameter reads `get('jchnooptimize' == '1')`, comparing the string to `'1'` before asking for it, so that parameter never worked at all.

## Which JCH Optimize versions are fixed?

| Line                       | Joomla element                | Joomla versions                                                    | Status                                     |
|----------------------------|-------------------------------|--------------------------------------------------------------------|--------------------------------------------|
| 9.4.0                      | <code>com_jchoptimize</code>  | 4.4 to 6.1 per the update feed, 5.0 or later per the release notes | Fixed                                      |
| 9.x before 9.4.0, 8.x, 7.x | <code>com_jchoptimize</code>  | Varies by release                                                  | Affected, update to 9.4.0                  |
| 6.5.0 and earlier          | <code>com_jch_optimize</code> | Almost entirely Joomla 3                                           | Affected as far as anyone has said, no fix |

### Joomla 4.4 sites: check before you update

The 9.4.0 release notes say it requires Joomla 5.0 or later, but the vendor's update feed still offers it to Joomla 4.4. If a Joomla 4.4 site updates and something breaks, roll back, and treat the Joomla 5 upgrade as the fix. mySites.guru flags those sites below 9.4.0 either way.

## What does this mean for Joomla 3 sites?

The old JCH Optimize line, version 6.5.0 and earlier, installs under a different element, `com_jch_optimize`, and nearly every site still running it is on Joomla 3. The vendor has said nothing about whether that code has the same flaws, and it has no fix. We have not added a rule for it, because we do not flag a version on a guess.

An optimiser that rewrites every page is a high-value place for a bug, and the old line gets no more security fixes. On a Joomla 3 site the practical choices are to uninstall JCH Optimize, or to make the move to a supported Joomla version that has been waiting. Our Joomla 3 extension vulnerabilities list tracks the other extensions in the same position.

## What to do today

1. Update JCH Optimize to 9.4.0 on each site running Joomla 4.4 or later, after confirming the site runs PHP 8.1 or later.
2. Check the component, the `system` plugin and the Page Cache plugin all report 9.4.0. A partly applied update leaves the old Page Cache endpoint in place.
3. Delete any JCH Optimize settings export you have saved, and rotate the Cloudflare API token and Redis password if an export ever left your hands.
4. On Joomla 3 sites, uninstall the old JCH Optimize line or plan the migration.
5. If you cannot update a site today, turn off the Page Cache plugin, which closes the unauthenticated endpoint.

## Beyond the version flag

A flag on a site card says a site is exposed. It does not tell you whether anyone used the hole first, and an XSS aimed at administrators is usually the first step towards an account an attacker should not have.

mySites.guru runs the follow-up checks as part of the subscription, unattended, on every connected site. The [rogue admin check](#) lists Super Users added outside the normal flow across your whole account in one view. The [Joomla malware scanner](#) looks for code dropped on the server. And the [vulnerable extension list](#) explains how version flags like this one work for every Joomla and WordPress extension we track.

If one of your sites already shows signs of compromise, work through [our Joomla hacked-site guide](#) or have us [fix it for you](#).

If you manage Joomla sites for clients, [mySites.guru](#) flags every connected site the day a fix like this ships, and the [free audit](#) shows what it finds on your own sites first.

---

## Further Reading

- [JCH Optimize 9.4.0 release notes](#) - the vendor's full changelog, with each fix rated HIGH, MEDIUM or LOW.
- [OWASP Cross Site Scripting Prevention Cheat Sheet](#) - output encoding, the rule an HTML optimiser has to respect when it rewrites a page.
- [OWASP Cross-Site Request Forgery Prevention Cheat Sheet](#) - why every state-changing admin request needs a token.
- [Joomla 3 extension vulnerabilities](#) - the Joomla 3 extensions with known holes and no vendor fix.

# Frequently Asked Questions

## **Which versions of JCH Optimize are affected?**

Every version before 9.4.0. The vendor ships one current release line and has not published a fix for any older branch, so 9.4.0 is the only fixed version. That covers the Free and Pro editions, which share the same version numbers.

## **Do any of these flaws need a login?**

Some do and some do not. The cross-site scripting issue, the Page Cache hit counter endpoint and the jchbackend parameter can all be reached by an anonymous visitor. The missing permission checks and the open redirect are in the administrator side, where an attacker needs either a lower-privileged backend account or a logged-in administrator who follows a crafted link.

## **Is there a CVE for the JCH Optimize 9.4.0 fixes?**

Not at the time of writing. The vendor rated six of the fixes HIGH in its release notes, but no CVE has been published and the release credits no finder. If a CVE is assigned later, mySites.guru will add the identifier to the same vulnerability rule.

## **Can I install JCH Optimize 9.4.0 on Joomla 3 or Joomla 4?**

Not on Joomla 3. The release notes say 9.4.0 needs PHP 8.1 and Joomla 5.0 or later, although the update feed still offers it to Joomla 4.4. Joomla 3 sites run the older JCH Optimize line, which installs under a different element and has no fix, so the realistic options there are to remove it or migrate the site.

## **Does JCH Optimize 9.4.0 break sites that use the Redis cache?**

Pro sites that use Redis as the cache store have reported a fatal error on every page after updating to 9.4.0, because the bundled Laminas Redis adapter is missing its Redis\Metadata class. Set the Storage Adapter to Filesystem before updating and switch back once the vendor ships a fixed build. The Free edition and Pro sites on Filesystem storage are not affected.

## **Is this a Joomla vulnerability?**

No. JCH Optimize is a third-party Joomla extension from Samuel Marshall, not part of Joomla itself. A Joomla site without JCH Optimize installed is not affected by any of these issues.

### How do I find every site running an affected JCH Optimize version?

By hand, you log in to each site and read its extension list. mySites.guru records every installed extension and its version on every connected Joomla site twice a day, and flags any site running JCH Optimize below 9.4.0 on its site card and in its audit.

**AI MODIFIED**

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

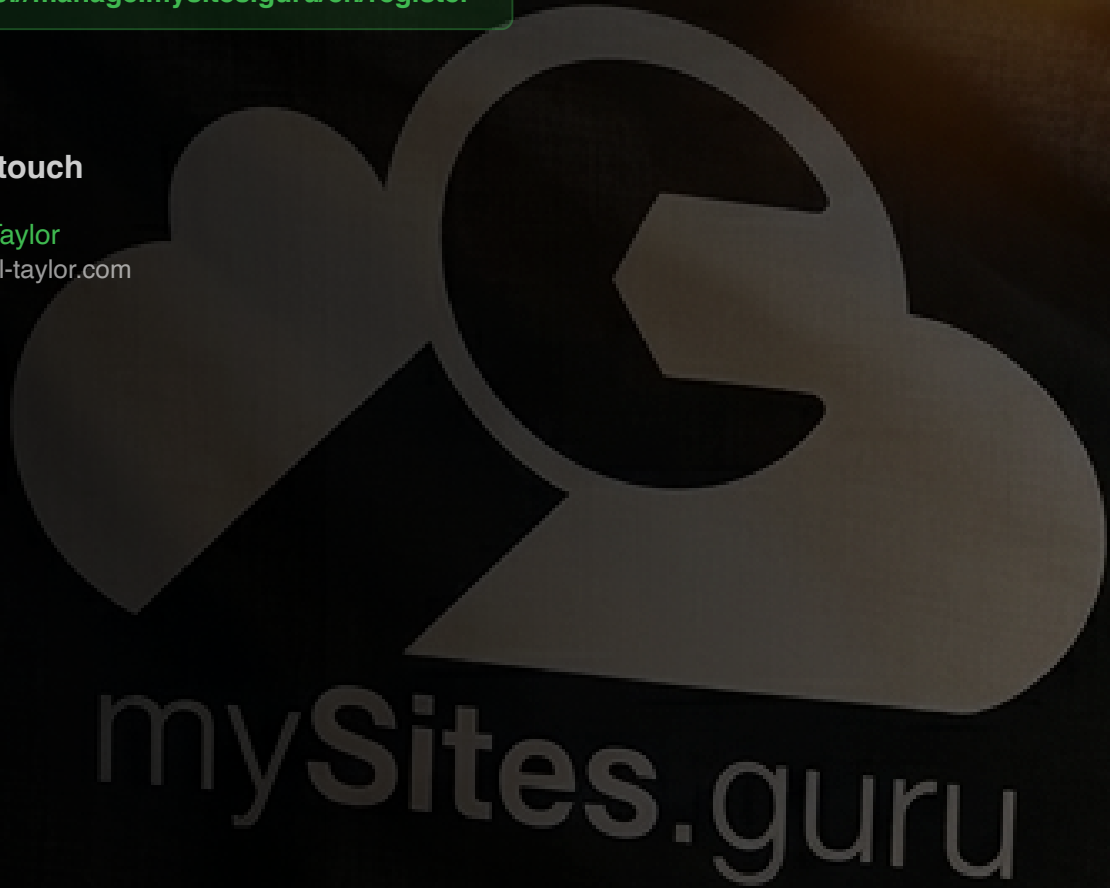
# Get Your Free Site Audit

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](mailto:phil@phil-taylor.com)



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

[mysites.guru](https://mysites.guru)