mySites.guru

JReviews 6.7.0 and 5.13.0 Stop Caching Secrets in a Public Folder

JReviews 6.7.0 and 5.13.0 stop writing the Joomla secret and API keys to a web-accessible cache file. What was exposed, who is affected and what to rotate.

Phil E. Taylor | 5 November 2026

ClickFWD released JReviews 6.7.0 for the v6 line and JReviews 5.13.0 for the v5 line on Wednesday 4 November 2026. Both changelogs list the same line under Security: “Stopped caching secret configuration values in a web-accessible file.” ClickFWD says nothing more: no CVE, no score, no researcher credit, no first affected version and no word on exploitation, and the list of modified files is only visible to signed-in subscribers. In JReviews 6.6.0, the release before the fix, running on Joomla 6, that cache file held the site’s Joomla secret and every third-party API key JReviews stores, in a folder inside the web root, with no login check in front of it.

JReviews is a commercial directory and reviews extension for Joomla, with a WordPress plugin alongside, made by ClickFWD LLC. The Joomla element is com_jreviews, and it runs on ClickFWD’s own framework, S2Framework (com_s2framework). This is a flaw in the Joomla extension and its framework, not in Joomla itself.

8.2
CVSS 4.0

JReviews below 5.13.0 and 6.7.0: secret configuration values in a web-accessible cache file

HIGH **mySites.guru assessment**

Anyone who knows the cache file name can download the cached JReviews settings without logging in, including the site's Joomla secret and any stored API keys.

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

No login needed | Exploitable over the internet | Needs the file name | Secrets exposed

▼ 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:P` Present: Needs a particular deployment or race to line up

PR:N None: No account needed
UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:H High: Everything the site holds 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 JReviews Was Caching, and Where

Before 6.7.0, JReviews loaded its full settings table and wrote it to the S2Framework cache. That cache lives at components/com_s2framework/tmp/cache/, inside the web root, and the settings copy sits in its core/ subfolder with jreviews_config in the file name. The file is plain serialized PHP data: an expiry timestamp followed by PHP serialize() output. It has no .php extension and no PHP guard at the top, so a web server hands it over as a plain download rather than running it, and the tmp folder has no .htaccess file, only empty index.html files.

An empty index.html stops a folder being listed by the web server. It does not stop a file in that folder being downloaded by anyone who knows its name, and there is no login check anywhere in the path. On a 6.6.0 install, the cached settings included:

- JReviews' own copy of the site's Joomla secret, the $secret value from configuration.php, held in a setting called cms_secret. JReviews fills it in automatically the first time it loads, and the cached value matched configuration.php exactly.
- The JReviews cron secret.
- Every third-party credential field JReviews has: Mapbox access token, ArcGIS client secret, Google Maps keys, Amazon S3 and DigitalOcean Spaces keys and secrets, reCAPTCHA and Cloudflare Turnstile secret keys, Facebook app secret, YouTube and Twitch keys, Transloadit and Zencoder keys.

Which of those hold a value depends on what the site configured. A directory site with maps and cloud storage set up has most of them filled in. The Joomla secret is there on every site, configured or not, because JReviews copies it on first load.

Why the File Name Is the Only Thing in the Way

The cache file cannot be fetched blind. Its name ends in a hash that includes the Joomla secret, so an attacker who only knows the folder path cannot guess the URL. That single condition is why our CVSS 4.0 assessment comes out at 8.2 High with attack requirements present (AT:P) rather than at a Critical score: the attacker needs the file name first.

An attacker has several ways to get that name. Directory listing switched on at the server (Apache's Options Indexes or nginx's autoindex), where the empty index.html is not served as the folder index, shows every file in the folder. A cache file name leaked anywhere gives the rest away, because every JReviews cache file with the same parameters shares that hash suffix. A backup or a copy of the site, left somewhere reachable, holds the file by name. And any other flaw that lets an attacker read or list files on the server turns a hashed name into a download link. None of those is exotic on a shared host with a few years of history behind it.

Which JReviews Versions Are Affected?

Treat any JReviews release before 5.13.0 on the v5 line or 6.7.0 on the v6 line as affected, along with everything older. ClickFWD gives no first affected version, and 6.6.0 is the only build we checked, so there is no version at which we can say the caching started.

JReviews version	Status	What to do
6.7.0	Fixed	Nothing beyond clearing the cache
6.0.0 to 6.6.x	Affected	Update to 6.7.0

JReviews version	Status	What to do
5.13.0	Fixed	Nothing beyond clearing the cache
5.x below 5.13.0	Affected	Update to 5.13.0, or move to 6.7.0
4.6.6 and older, including Joomla 3 sites	Affected, no fixed release	Move to a supported line; block the folder meanwhile

Both releases also list other security items. In 6.7.0, ClickFWD “Blocked new reviews on inaccessible listings and external records” and “Fixed forms losing their abuse-protection token after an error”. In 5.13.0 it “Fixed legacy detail pages loading unpublished listings and frontend listing queries including unpublished media” and “Blocked invalid custom-field sort values in listing queries”. Both releases fix helpful votes and deletions failing because legacy pages sent the wrong security token. None of those comes with any more detail than the caching line did.

What To Do on Every JReviews Site

1. Update JReviews to 6.7.0 on the v6 line or 5.13.0 on the v5 line, through the Joomla updater or JReviews’ own installer.

2. Clear the JReviews cache from the JReviews control panel, which has a clear-cache action. The fix stops new cache files being written; it does not by itself prove a file written before the update has gone, so make sure. Then look in components/com_s2framework/tmp/cache/ for any file with jreviews_config in the name and confirm none is left.

3. Block web access to components/com_s2framework/tmp/ at the server, whatever version you run. The folder has no reason to be fetchable from a browser. On Apache, a .htaccess file in that folder:

   ```
   Require all denied
   ```

On nginx, a location block in the site's server config:

```
location ^~ /components/com_s2framework/tmp/ { deny all; }
```

4. If the file could have been exposed, because the site has had directory listing on, a backup in a reachable place, a cache file name in a log or a report, or another flaw, rotate what it held. Change the Joomla secret in configuration.php, which signs everyone out. Regenerate the JReviews cron secret. Rotate every third-party key held in JReviews settings at its provider: Mapbox, S3, Spaces, the CAPTCHA services and the rest.

> **Changing the Joomla secret does not change JReviews' copy**
>
> JReviews keeps its own copy of the Joomla secret in its cms_secret setting and uses that copy for its own hashing, such as ID hashes and guest identities. Rotating $secret in configuration.php leaves cms_secret holding the old value. Ask ClickFWD how to rotate it before editing cms_secret directly, since the extension's own hashes are built from it.

Joomla 3 JReviews Sites Have No Fix

The JReviews 4.x line stopped at 4.6.6 on 25 July 2024, and ClickFWD has not released a fixed version for it. The vendor's requirements page lists Joomla 4, 5 and 6 and WordPress 6.x as the supported platforms, so a Joomla 3 site running JReviews has nothing supported to update to. The same goes for any site still on 4.x or older on a newer Joomla.

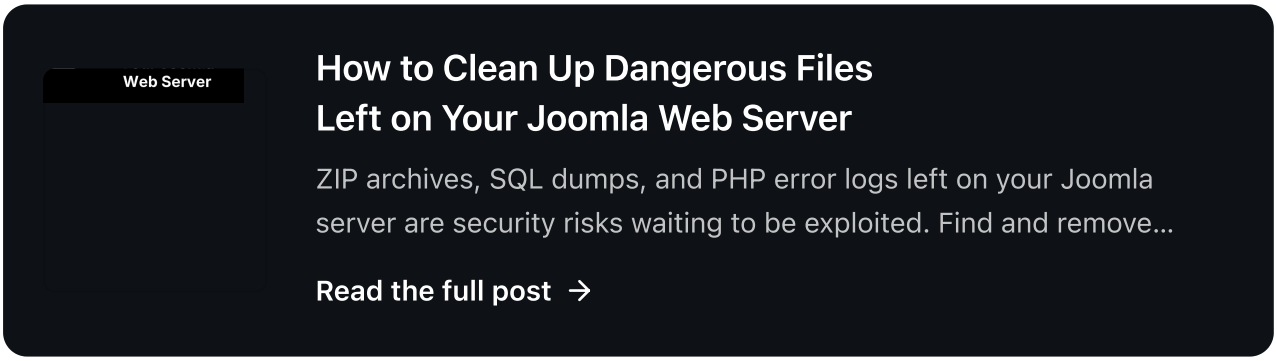
The route out is a move to a supported JReviews line on Joomla 4 or later. Until then, the server-level block in step 3 above is the main protection, because it stops the download whether or not the file name ever leaks, and the rotation advice in step 4 applies in full.

How mySites.guru Flags JReviews

On 5 November 2026 we added two rules that flag every connected Joomla site running JReviews (com_jreviews) below 5.13.0, or 6.x below 6.7.0. On release day, 100% of the Joomla sites with JReviews that we monitor were on an affected version, spread across every line from 2.x up to 6.6.0, with 6.6.0 the largest single group. The flag shows on each site's dashboard and in its vulnerable extension list, alongside the security release flag that marks extension updates with a security fix in them. The JReviews WordPress plugin is not covered by this Joomla rule; WordPress flags come from our Wordfence-based feed.

JReviews is a commercial extension, so update it through the Joomla updater or JReviews' own installer, then use the same dashboard that drives bulk updates to see which sites still show the flag after you have worked through them. Every rule we hold is listed on the public vulnerabilities page, and the flags are part of the subscription.

A cache file full of secrets is one more reason to keep the web root clear of files that have no business being reachable from a browser, stale or otherwise.



If a site has already been hit, or you would rather someone else made sure, fix.mySites.guru patches the site, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Further Reading

- JReviews changelog, v6 line - the 6.7.0 release notes with the one-line security entry.
- JReviews changelog, v5 line - the 5.13.0 release notes with the same entry.
- JReviews requirements - the vendor's supported CMS versions: Joomla 4, 5, 6 and WordPress 6.x.
- The Vulnerable Extension List for Joomla and WordPress - how the flag for this release reaches every connected site.
- How to Clean Up Dangerous Files on a Joomla Server - finding and removing files that should never sit in the web root.

Frequently Asked Questions

Which JReviews versions fix the cached secrets flaw?

JReviews 6.7.0 on the v6 line and JReviews 5.13.0 on the v5 line, both released by ClickFWD on 4 November 2026. Every older release on either line should be treated as affected. The 4.x line ended at 4.6.6 in July 2024 and has no fixed release, which also means a Joomla 3 site has nothing supported to update to.

Is there a CVE for the JReviews 6.7.0 security fix?

No. ClickFWD gives no CVE, no CVSS score, no researcher credit and no first affected version, and says nothing about whether the flaw was exploited. The list of modified files is only visible to signed-in subscribers. No CVE has been assigned at the time of writing. The 8.2 High score in this post is our own CVSS 4.0 assessment, not the vendor's.

What was in the JReviews cache file?

A copy of the whole JReviews settings table, as serialized PHP data. That includes JReviews' own copy of the site's Joomla secret, the JReviews cron secret, and every third-party credential field the extension has: Mapbox, ArcGIS, Google Maps, Amazon S3, DigitalOcean Spaces, reCAPTCHA, Cloudflare Turnstile, Facebook, YouTube, Twitch, Transloadit and Zencoder keys. Which of those hold a value depends on what the site configured.

Can anyone just download the JReviews cache file?

Not blindly. The file sits in the web root with no login check and no PHP guard, but its name ends in a hash that includes the Joomla secret, so an attacker cannot guess the URL. It becomes reachable when something else gives the name away: directory listing switched on at the server, a cache file name leaked anywhere, a backup or copy of the site, or another flaw that lets an attacker read or list files.

What should I rotate after updating JReviews?

Only if you believe the file could have been exposed. Change the Joomla secret in configuration.php, which signs everyone out; regenerate the JReviews cron secret; and rotate every third-party key held in JReviews settings at the provider. JReviews keeps its own copy of the old Joomla secret in its cms_secret setting and uses it for its own hashing, so changing the Joomla secret does not change that copy. Ask ClickFWD before editing cms_secret directly.



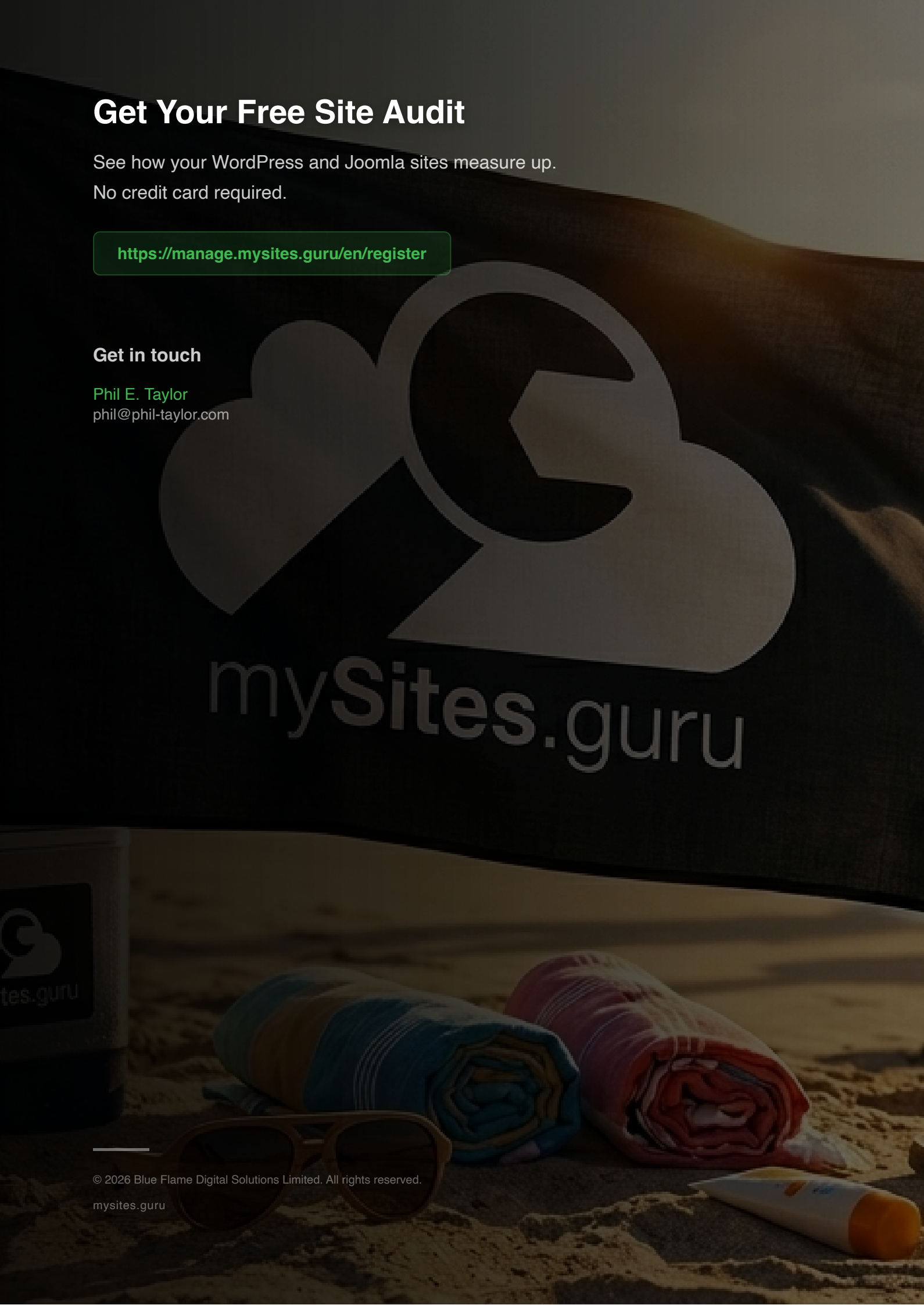
Written and edited by a human, with AI assistance. Our approach to AI

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.