mySites.guru

JCE 2.9.99.10 Fixes Another Security Issue

JCE 2.9.99.10 patches a file rename flaw that let a privileged user create a hidden file in the folder they were browsing. The release also hardens far more than its changelog lists.

Phil E. Taylor | 29 July 2026

Active Joomla Extension security alerts: Nineteen and counting this month • Helix3 defacements • JCE • EasyStore • Regular Labs • Gridbox

JCE (Joomla Content Editor) ships on more Joomla sites than any other editor extension, and it sits in the top two of our live extension ranking. On 29 July 2026 the developer released JCE 2.9.99.10 with one item in the changelog marked SECURITY.

That item is a small one, and saying so plainly matters more than manufacturing urgency. An authenticated user with a privileged editor profile could rename a file so that it became hidden in the folder they were browsing. It needs a login, a profile that grants file browser access, and the Rename permission on top of that. It is not remote code execution and it is not another June.

If you manage Joomla sites in bulk, mySites.guru already indexes every extension on every connected site, so finding everything below 2.9.99.10 and pushing the update across all of them is a two-step job rather than an afternoon of logging into administrator panels. The JCE Profiles Hack page remains the page of truth for the far more serious June attack, which is still the reason most Joomla sites need attention.

The short version

JCE 2.9.99.10 fixes an authenticated, privileged-user file rename flaw that could create a hidden file. No CVE assigned as of 29 July 2026. It is a routine update, not an emergency. The genuinely urgent JCE problem was fixed back in 2.9.99.5, and any site still below that release is the one to worry about.

TL;DR

- **JCE 2.9.99.10** released 29 July 2026, with one changelog item marked SECURITY
- An **authenticated, privileged user** could rename a file so it became hidden in the folder being browsed
- Rename also no longer silently **replaces a file that already exists**

- **No CVE** assigned as of 29 July 2026
- Materially less severe than **CVE-2026-48907**, the unauthenticated flaw fixed in 2.9.99.5 and later added to CISA's Known Exploited Vulnerabilities catalog
- Comparing the two packages shows the release **hardens considerably more than the changelog lists**
- Update at your normal cadence, but treat anything **below 2.9.99.5** as urgent

What JCE 2.9.99.10 actually fixes

The vendor describes the security item in one sentence: an authenticated, privileged user could rename a file in a way that created a hidden file in the folder they were browsing, instead of the rename being rejected as invalid. The release notes add that renaming will no longer replace a file that already exists, which is a second, quieter fix bundled into the same change.

Three conditions have to hold before any of that is reachable. The attacker needs a working login, a JCE editor profile assigned to them that grants file browser access such as the Image Manager or File Browser, and the Rename permission within that profile. On a site where lower-trust users get an editor profile with file management turned on, that is a realistic combination. On a site where only administrators touch the file browser, it is not.

The outcome is a hidden file, not code execution. The extension of the renamed file is inherited from the original, so an attacker cannot choose it. A file called `photo.jpg` can be turned into `.jpg`, which disappears from the JCE file listing and from a plain directory listing on the server. That is a concealment trick, useful for hiding something already uploaded, rather than a way of getting anything new onto the server.

Is this as serious as the June JCE vulnerability?

No, and conflating the two would be a disservice. June's issue was CVE-2026-48907: unauthenticated, CVSS 10.0, exploitable by anyone who could reach the site, and

added to CISA's Known Exploited Vulnerabilities catalog after evidence of real-world attacks. It was fixed in 2.9.99.5 on 3 June, followed by a full hardening audit in 2.9.99.6.

The 2.9.99.10 issue sits at the opposite end of the scale. It needs authentication, a privileged profile, and a specific permission, and it yields concealment rather than execution. No CVE had been assigned as of 29 July 2026, which is a reasonable outcome for a bug of this shape reported privately to a developer who patched it.

What makes it worth attention at all is scale. JCE is the most widely installed Joomla editor, so a file handling weakness in it reaches a lot of sites if it ever chains with something else.

What the JCE changelog does not mention

We unpacked both release packages and compared them file by file. Of the eight sub-packages inside `pkg_jce`, only `com_jce` contains real code changes; the seven bundled plugins are version bumps and nothing else. Within `com_jce`, most changed files differ only in their version banner, leaving a much smaller set of genuine changes.

Several of those changes are substantive security hardening that appears nowhere in the changelog:

- The blocked executable extension list grew a lot. 2.9.99.10 adds `pht`, `phtm`, `phps`, `phpt`, `pgif`, `aspx`, `asa`, `asax`, `cer`, `jsp`, `jspx`, `cgi`, `pl`, `inc`, `shtml`, `shtm`, `stm`, `htaccess`, `htpasswd` and `ini`. None of those were blocked in 2.9.99.9.
- Each part of a filename is now trimmed of colons and semicolons before comparison, and the whole name is Unicode normalised. That defeats classic bypass shapes such as `shell.php:.jpg` and fullwidth-character variants.
- The random filename suffix went from five hexadecimal characters of an md5 of `uniqid(rand(), 1)` to sixteen characters from `random_bytes()`. The changelog

mentions the new fully-randomised naming option, but not that the old generator was guessable.

- Rename, copy and move now validate file extensions. Previously only the filename was checked on those operations, not whether the extension was permitted by the profile.
- The `allowroot` filesystem option is gone. In 2.9.99.9, setting it pointed the file browser at the site root rather than the configured images directory.

None of that is criticism of the developer, who has shipped seven releases on this extension since May and has been open about the June incident. But it does mean the changelog understates what this release is. If you were deciding whether to bother, decide on the hardening rather than the one listed item.

Which Joomla sites are actually affected?

Across the Joomla sites connected to mySites.guru, not one is running a version in the affected 2.9.99.6 to 2.9.99.9 window. Sites that stay close to current move through these releases fast, and the handful sitting on a 2.9.99.x build had already gone past it.

The uncomfortable half of the same data is that hundreds of connected Joomla sites are still on a 2.7.x build of JCE, years behind, and a long tail sits on 2.6.x and older 2.9.x releases. Those sites are not exposed to the rename issue. They are exposed to the unauthenticated upload flaw that CISA confirmed was being actively exploited, which is a far worse place to be.

If you look after Joomla sites for other people, that gap is the thing to plan around. The sites that need your attention are almost never the ones a release behind. They are the ones nobody has touched since the last redesign.

How do I update JCE across every Joomla site?

On a single site, update JCE the way you would any Joomla extension, through the Joomla Update or Extensions manager in the administrator. JCE 2.9.99.x runs on Joomla 3, 4, 5 and 6, and the developer confirms it does not need the Backwards Compatibility plugin on Joomla 5 or 6.

Across many sites, doing that by hand does not scale, which is the problem mySites.guru exists to solve. Every connected Joomla site has its full extension inventory indexed, so you can list every site with JCE installed grouped by version, identify everything below 2.9.99.10, and push the update across all of them in one batch. The free audit will show you the same inventory for your own sites before you commit to anything.

While you are in there, it is worth checking older sites for the traces of the June attack rather than assuming an update is a cleanup. Updating an extension closes the hole; it does not remove anything that came through it. Our guide to finding every site running a vulnerable JCE covers the indicators of compromise and the tool that finds rogue profiles.

If you cannot update JCE straight away

The developer has published a specific interim measure for this issue, which is unusual and welcome. Disable the Rename option in the settings of each file-related plugin, such as the Image Manager and the File Browser, for any profile assigned to untrusted or lower-trust users. That removes the permission the flaw depends on until the update is applied.

> **Warning**
>
> This mitigation applies to the rename issue only. It does nothing for the unauthenticated upload flaw fixed in 2.9.99.5. If a site is below 2.9.99.5, no permission change will protect it, because the attack does not need a login at all.

The broader point the developer makes alongside it is the right one, and it applies well beyond JCE. The features and access you grant to lower-trust users on any Joomla

extension should be the minimum they actually need, reviewed occasionally rather than set once and forgotten. Most file browser permissions in the wild were granted years ago to someone who has since left.

Does this affect WordPress?

No. JCE is a Joomla-only editor extension. There is no WordPress build and no shared codebase, so WordPress sites running the block editor or TinyMCE are unaffected by this release and by every other JCE issue covered here.

Further Reading

- JCE Pro 2.9.99.10 released - the developer's own announcement, including the interim mitigation for sites that cannot update immediately.
- JCE Editor changelog - the full version-by-version history, useful for seeing how many releases a site has skipped.
- CVE-2026-48907 on NVD - the record for the unauthenticated flaw fixed in 2.9.99.5, the one that actually matters for older sites.
- CISA Known Exploited Vulnerabilities catalog - CISA only lists a flaw here with evidence of exploitation in the wild.

Frequently Asked Questions

What does JCE 2.9.99.10 fix?

JCE 2.9.99.10, released 29 July 2026, fixes a file rename flaw in the editor's filesystem functions. An authenticated user with a profile granting file browser access and the Rename permission could rename a file so it became a hidden file in the folder being browsed, rather than the rename being rejected as invalid. The same release also stops a rename silently replacing a file that already exists.

Is JCE 2.9.99.10 as serious as the June JCE vulnerability?

No, and the difference matters. The June issue, CVE-2026-48907, was unauthenticated, scored CVSS 10.0, and was added to CISA's Known Exploited Vulnerabilities catalog after real attacks. It was fixed in 2.9.99.5. The 2.9.99.10 issue requires an existing login, a JCE profile that grants file browser access, and the Rename permission on top. It produces a hidden file, not code execution. If you are already on 2.9.99.5 or later you are not in a fire drill.

Has a CVE been assigned to the JCE 2.9.99.10 issue?

No CVE had been assigned as of 29 July 2026, the day the release shipped. That is unsurprising for an authenticated, privileged-user-only issue reported directly to the developer. The absence of a CVE is not a reason to skip the update.

Which JCE versions are affected by the rename issue?

The rename fix applies to 2.9.99.6 through 2.9.99.9. Anything below 2.9.99.6 has a much more serious problem, namely the unauthenticated upload flaw patched in 2.9.99.5, so those sites need updating urgently for a different reason. Every version below 2.9.99.10 should be brought up to the current release.

What can I do if I cannot update JCE straight away?

The developer's own interim advice is to disable the Rename option in the settings of each file-related plugin, such as the Image Manager and File Browser, for any profile assigned to untrusted or lower-trust users. That blocks the affected operation until you can apply the update. It is a stopgap, not a substitute for updating.

Does JCE 2.9.99.10 require the Joomla Backwards Compatibility plugin?

No. The developer states that JCE 2.9.99.x is compatible with Joomla 3, 4, 5 and 6, and

does not require the Backwards Compatibility plugin on Joomla 5 or Joomla 6.

Does this JCE issue affect WordPress?

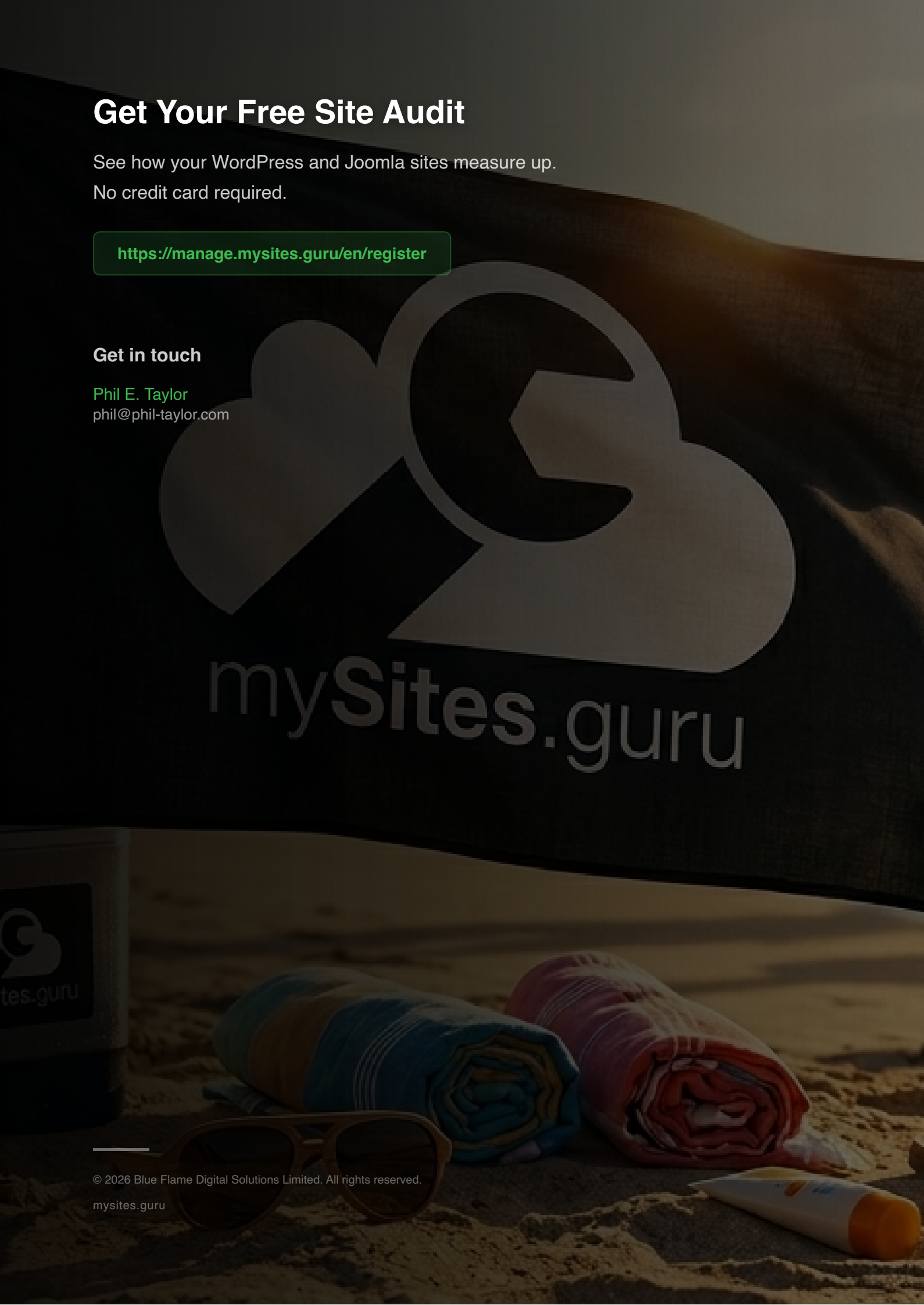
No. JCE is a Joomla-only editor extension with no WordPress build and no shared codebase. WordPress sites are unaffected by this release.

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