



The Joomla Content Editor (JCE) Hack, Four Months On

Four months after the JCE hack hit Joomla sites, unpatched installs are still being compromised. See the damage and how mySites.guru finds and fixes it.

Phil E. Taylor | 20 October 2026

It is four months since the JCE hack tore through Joomla sites in June 2026. The flaw in the JCE editor is patched, the headlines have moved on, and the attack has not. Unpatched JCE installs are still being compromised today, and mySites.guru is still finding fresh ones.

If you run Joomla sites for clients and have not checked every one of them since June, this post is for you. The full indicators of compromise, the find-and-fix tool and the complete timeline are on [our JCE hack page](#). This is the shorter version: what happened, what a hit looks like, and proof the watching has not stopped.

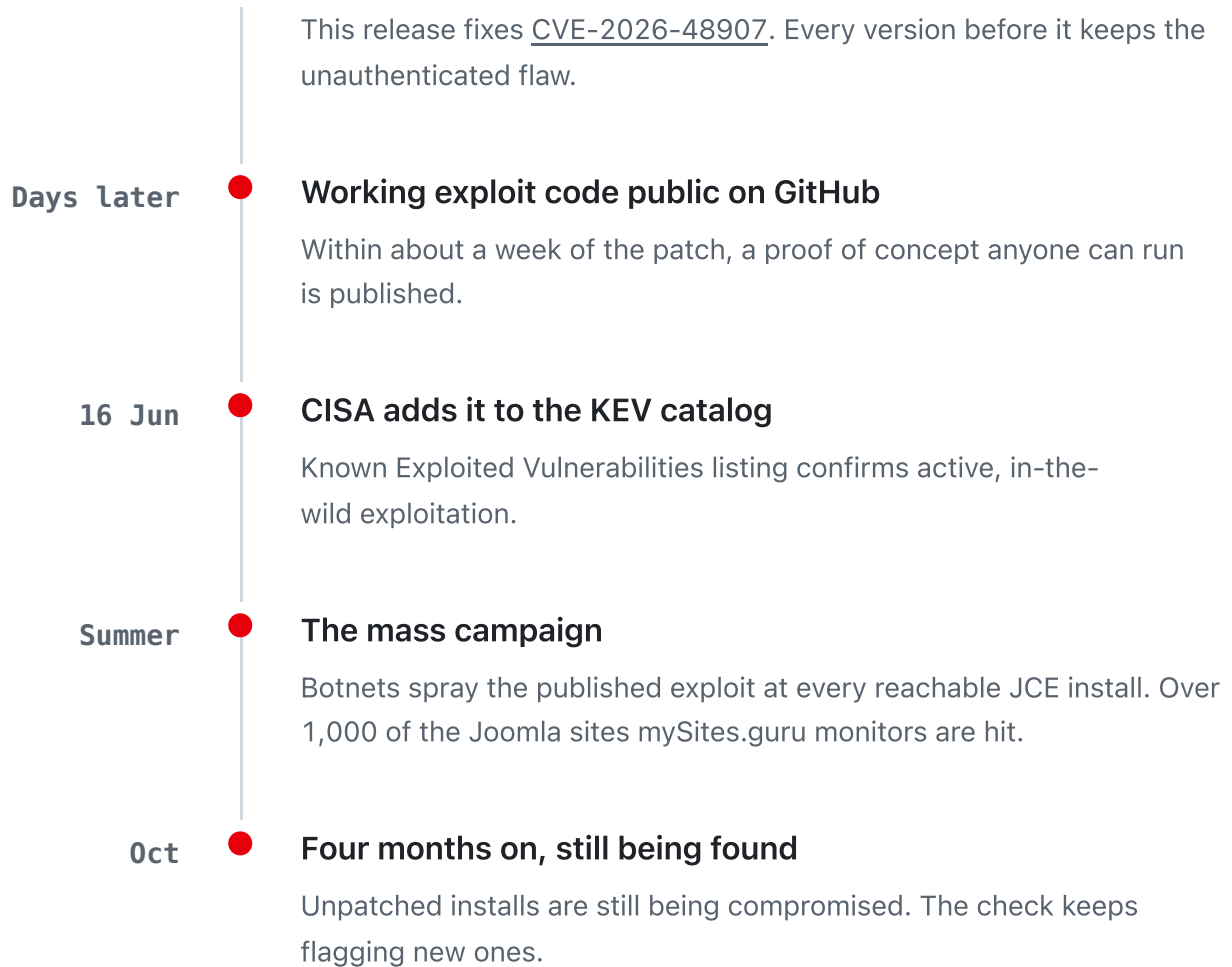
What is the JCE hack?

JCE (Joomla Content Editor) is the most-installed editor extension on Joomla, sitting in the top two of our [live extension ranking](#) neck and neck with Akeeba Backup. [CVE-2026-48907](#) is an improper-access-control flaw in the JCE extension that let an unauthenticated visitor import an editor profile and use it to upload and run PHP. The Joomla project, as CNA, rated it 10.0 Critical on CVSS 4.0; NVD scored it 9.8. No login is required at any step.

The chain is short. The attacker posts a rogue editor profile with a large negative ordering (-99999 is typical) so it floats above every real profile. That profile allows php and txt uploads with MIME validation switched off. A second request uploads a webshell through the JCE file browser. Two requests, no credentials, fully automated. The fix was released in [JCE 2.9.99.5](#) on 3 June 2026, and the [June pillar post](#) walks through every step at length, so I will not repeat it here.

How the JCE hack unfolded





What we are still finding today

Numbers first, from the 24 hours before I wrote this.

16,464

rogue JCE editor profiles found and verified, last 24 hours

21,552

malicious files found and verified, last 24 hours

1,000+

Joomla sites we have found hit by this attack

100,000+

connections checked daily

The first three are confirmed findings, not estimates: in a single day the JCE check flagged and verified that many rogue profiles and malicious files across the Joomla sites we monitor, spread over the thousand-plus sites this attack has hit. The fourth is the scale behind them. We check more than 100,000 site connections a day, so a fresh compromise shows up on the next snapshot rather than whenever someone next happens to log in. Four months on, the numbers are not shrinking, because the long tail of unpatched sites keeps feeding them.

The check is called Check for JCE Rogue Profiles & Backdoors. It runs on every snapshot, twice a day, on every connected Joomla site. It finds the rogue profiles and the webshells automatically, and when it flags something you fix it from one screen: remove the rogue profiles, delete the backdoor files and update JCE, on Joomla 4, 5 and 6. It never deletes anything on its own. It lists everything first so you can take a copy for evidence before you clean.

To find every still-vulnerable install, the extension search lists every site running JCE grouped by version, and the mass updater patches them all in one batch. Twenty sites or two hundred, it is one job.

How far the JCE hack reached

This was never a story about neglected sites with no one watching them. In June the attack took down the Joomla project's own flagship sites at once: the official Joomla Extensions Directory at extensions.joomla.org, community.joomla.org and certification.joomla.org all served "503 Maintenance" pages. Those sites are run by people who know Joomla security better than almost anyone.

That is the whole point. JCE is installed so widely that any site running an old copy was exposed, and competence did not protect you. An exploit that needs no login hits every reachable install in the same sweep, and the only thing that mattered was whether your JCE was patched before the bots reached it. No amount of .htaccess hardening stood in the way either, because the requests look like ordinary POSTs to an extension the site is supposed to serve.

How to tell if your Joomla site was hit

The rogue profiles are easy to recognise once you know the shape. Most have machine-generated names: a capital J followed by six digits, J940401, J938560 and so on. Some attackers did not bother with subtlety and named theirs "Pwned" with the description "RCE via JCE". If a profile like that sits at the top of your JCE profiles list, you have been hit.

The webshells were dropped in tmp, media, images and the libraries tree: hidden .xml.php droppers, eval(gzinflate(base64_decode(...))) blobs, shell_exec command shells and small "Nxploited" marker files. Our [backdoor scanner](#) picks these up, and so does the dedicated JCE check described above.

The access logs give it away in two lines: a POST to task=profiles.import that creates the profile, then a POST to method=upload that drops the shell. Both return 200, both unauthenticated. The requests came from many different IPs with python-requests user agents. This was a botnet spraying a published exploit, not a targeted attack, which is why one vulnerable site is almost never the only one in a portfolio. mySites.guru has now found this attack on over 1,000 of the Joomla sites it monitors.

Is the JCE hack still a threat?

Only if you are running an old version. A fixed CVE is a closed chapter for the sites that updated. For the long tail that did not, the chapter is still open, which is exactly why we are still finding this four months on. The exploit code is public, the bots never stopped, and every Joomla site still on a vulnerable JCE is as exposed today as it was on 3 June.

If this feels familiar, it should. In 2012 the JCE ImageManager flaw (CVE-2012-2902) let unauthenticated visitors upload files through JCE, and automated bots kept exploiting it for years after the patch existed, purely because so many installs were never updated. The patch fixed the software; it did nothing for the sites that never installed it.

The JCE hack was a starting gun

Days after the JCE hack, a friend told me Joomla extensions were more secure than WordPress plugins. I disagreed. The gap is attention, not security. WordPress plugins have bug-bounty programmes and a black market that pays for working exploits, so thousands of researchers pick at them. Almost no one scrutinises Joomla extensions with the same intent.

So we went looking. Between mid-June and late July, mySites.guru found and privately disclosed 19 vulnerabilities across 17 Joomla extensions, written up in [Nineteen and Counting](#). For over a week it was one or two critical, mostly unauthenticated remote-code-execution flaws a day.

That was just the first month. Four months on the count is well past nineteen and still climbing, and we are holding more that we cannot name until their vendors patch.

The bugs were always there. No one was looking. The JCE hack made people look, and it has pushed Joomla extension developers to take security more seriously.

The worst extension flaws we have found since

The worst ten, the critical and mostly unauthenticated ones. The four marked in red were being exploited in the wild, so CISA added them to its Known Exploited Vulnerabilities catalog.

15 Jun		<u>iCagenda: unauthenticated upload RCE (CISA KEV)</u>
15 Jun		<u>SP Page Builder: zero-day RCE, fake admins planted (CISA KEV)</u>
27 Jun		<u>Page Builder CK: unauthenticated upload RCE (CISA KEV)</u>

8 Jul	●	<u>Balbooa Forms: unauthenticated upload RCE (CISA KEV)</u>
9 Jul	●	<u>AcyMailing: unauthenticated SQL injection, every user record and hash exposed</u>
10 Jul	●	<u>RSFiles!: unauthenticated file upload RCE, CVSS 10.0</u>
20 Jul	●	<u>Gridbox: one cookie and you are a Super User, CVSS 10.0</u>
19 Aug	●	<u>YOOtheme ZOO: an unauthenticated upload, CVSS 10.0</u>
22 Aug	●	<u>Fabrik 4.7.2: a long list of fixes, up to CVSS 10.0</u>
26 Sep	●	<u>UP plugin: file read and code execution, CVSS 10.0</u>

Another two dozen sit in the [full disclosure archive](#), every one found by us and reported privately before it went public.

Is JCE safe to use?

JCE is not the cautionary tale in this post. Ryan Demmer of Widget Factory has developed it since 2006, it is the most-installed editor on Joomla, and it is a mature, carefully engineered extension. When [CVE-2026-48907](#) came out, the response was the one every vendor should copy: the fix in 2.9.99.5 within days, a four-day audit of the whole editor and a hardening release (2.9.99.6) within a week, a run of further security and maintenance releases after that, a free patch for sites stuck on end-of-life PHP or Joomla, and a clear public advisory. One bad bug, owned fast and thoroughly.

Not every Joomla extension is run like that. Since the JCE hack we have had to report critical, mostly unauthenticated flaws in the same products again and again. [SP Page Builder](#) is the clearest case: five separate disclosures from us in four months. Some

vendors patch fast and completely, as Ryan Demmer did. Others leave the same class of hole open release after release. A good extension is one whose developer responds like that when it matters, and the real risk is the long tail whose vendors do not. That is the whole reason to have every site watched.

I patched JCE. Am I still at risk?

Patched is not the same as clean. If a site ran a vulnerable JCE for any length of time before it was updated, it could already have been compromised, and a webshell sitting on disk does not care that the entry point is now shut. Updating closes the door; you still have to check whether anyone walked through it first.

Patching in June does not mean the site is clean

A rogue profile planted before the update is still in the profiles list after it. A webshell dropped in tmp or media still answers requests after it. Check every site that ever ran a vulnerable JCE, whatever version it runs now, and treat a clean result as today's result rather than a permanent one.

That is the argument in [hacked yesterday, exploited today](#): a one-off cleanup is a snapshot, and only ongoing monitoring tells you a site is still clean next week.

Which JCE version is safe?

The rule is simple: if your JCE is anything below 2.9.99.5, the unauthenticated profile upload ([CVE-2026-48907](#)) is open on your site, and that covers every Free and Pro release back through the 2.8.x and 2.7.x branches.

JCE version	Where it stands
2.9.99.4 and earlier (incl. 2.7.x, 2.8.x)	Vulnerable: the unauthenticated profile-upload flaw
2.9.99.5 to 2.9.99.11	Patched, but superseded

JCE version	Where it stands
2.9.99.12	Current, for Joomla 3 and 4
3.0.2	Current, for Joomla 5 and 6 (needs PHP 8)
2.6.x	Not affected by default, but unsupported: migrate

Update to whichever current release matches your Joomla and PHP version. If the site is stuck on end-of-life PHP or Joomla and cannot take that update, the JCE developer has published a [free security patch package](#) covering 2.7.x, 2.8.x and 2.9.x. Treat it as a stopgap. It closes this one flaw and nothing else, and it does not clean a site that was already compromised before you applied it.

Why mySites.guru matters when a hack like this breaks

If you run a digital agency, the worst phone call you can get is a client telling you their site has been hacked. The sting is not the fix, it is that they knew before you did. mySites.guru exists to prevent that call.

Every client site you look after connects through a lightweight connector, and from then on a snapshot runs on every site twice a day. So when a hack like this breaks, you do not log into each admin panel one by one to work out who is exposed. You open [extension search](#) and within seconds you have every connected site running JCE, grouped by version. You can pinpoint which sites are affected, decide which to fix first and how fast, and get ahead of it before your clients even know there was a problem. That triage is simple when every site is in a single tool, and slow and error-prone when it is not.

Fixing is just as quick. The [mass updater](#) upgrades JCE across every affected site in one batch, or reinstalls a clean copy over the top. Enrol the extension in automatic overnight updates and the next release goes on without you lifting a finger. Then run a full audit: hundreds of checks per site, including hacked-site detection for rogue JCE profiles, rogue admins, suspect content and webshells, with clear guidance on every finding and help from us throughout.

If you would rather hand the whole thing over, fix.mysites.guru is a flat £120 per incident, usually done the same day. We screen the site first, so you are not charged if we cannot fix it, and non-subscribers get a free month on top.

I have been doing this since 2012. Fourteen years, 90,000+ sites protected, 1,000,000+ audits completed, and I will say it straight: no other platform brings this combination of Joomla expertise, support and toolset to a moment like this. One subscription covers [unlimited sites](#).

[Connect your first site free](#). No card, about two minutes.

Further Reading

- [The JCE hack: indicators of compromise, timeline and the find-and-fix tool](#) - our page of truth for this attack
- [Finding every site running a vulnerable JCE](#) - the full technical walkthrough from June
- [Nineteen and Counting: Joomla extension vulnerabilities we found in a month](#) - the wave of disclosures the JCE hack set off
- [JCE security update and a free patch for older sites](#) - the JCE developer's own advisory, confirming active exploitation and announcing the free patch package
- [Active exploitation of JCE Editor CVE-2026-48907](#) - independent confirmation of the mass-exploitation campaign from ChronoEngine, July 2026
- [CVE-2026-48907 at cve.org](#) - the CVE record

The June pillar post has the full technical walkthrough; the links below are the primary sources this recap draws on.

Frequently Asked Questions

Is the JCE hack still a threat four months later?

Yes. The flaw in the JCE extension ([CVE-2026-48907](#)) was fixed in June 2026, but the exploit code is public and automated bots are still spraying it at every reachable Joomla site. Any install still on JCE 2.9.99.4 or earlier is as exposed today as it was on the day the patch was released, and mySites.guru is still finding fresh compromises on the Joomla sites it monitors.

I updated JCE in June. Could my site still be compromised?

Yes, if it ran a vulnerable version for any length of time before you updated. The update closes the entry point, but it does not remove a rogue editor profile or a webshell that was planted while the door was open. You need to check the JCE profiles list and the usual drop folders (tmp, media, images and libraries), or let a dedicated check do it for you.

How do I check every Joomla site I manage at once?

Connect them to mySites.guru. The extension search lists every site running JCE grouped by version, so the still-vulnerable ones are obvious in one screen, and the mass updater patches them in one batch. Separately, the "Check for JCE Rogue Profiles & Backdoors" check runs on every snapshot, twice a day, and flags any site with a rogue profile or a planted webshell.

Does mySites.guru remove the JCE hack or just detect it?

Both. The check finds the rogue profiles and the backdoor files automatically. When it flags something, you remove the rogue profiles, delete the backdoor files and update JCE from one screen, on Joomla 4, 5 and 6. It never deletes anything on its own: it lists everything first so you can take a copy for evidence.

Which JCE version is safe from CVE-2026-48907?

JCE 2.9.99.5 and every release after it. Anything on 2.9.99.4 or earlier still has the unauthenticated flaw. As of October 2026 the current releases are JCE 2.9.99.12 for Joomla 3 and 4, and JCE 3.0.2 for Joomla 5 and 6 (JCE 3.0 needs Joomla 5+ and PHP 8+).

AI MODIFIED

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

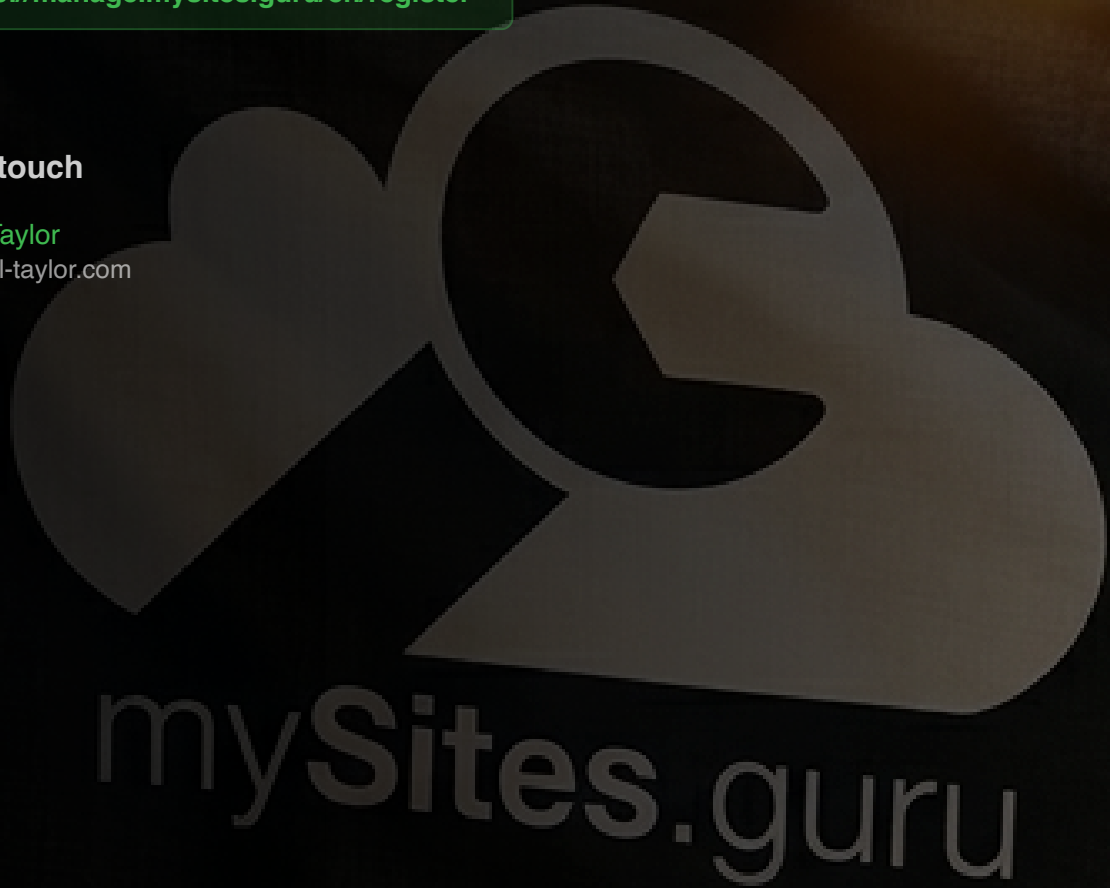
Get Your Free Site Audit

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