mySites.guru

Custom Tables for Joomla: Unauthenticated File Upload Fixed in 3.7.8

CVE-2026-105606: anyone can upload a file to a Joomla site's tmp folder through a public Custom Tables form. Scored 9.5 Critical, fixed in Custom Tables 3.7.8.

Phil E. Taylor | 3 November 2026

Custom Tables 3.7.8 fixes an unauthenticated file upload in the Joomla extension by JoomlaBoat. The Joomla CNA published it as CVE-2026-105606 on 2 November 2026, scored CVSS 4.0 9.5 Critical, under the title "Unauthenticated arbitrary file upload in Custom Tables < 3.7.8". Every version from 1.0 to 3.7.7 is affected, and the fix is 3.7.8. The flaw is in the extension, not in Joomla itself, and it is the second JoomlaBoat extension flaw we have covered this year, after the YouTube Gallery SQL injection.

The exposed sites are the ones that show a public Custom Tables submission form with a file field. On those, any visitor can push a file with an extension of their choosing into the site's temp folder, with no login and no account, and the response tells them where it went. If you manage a Joomla site running Custom Tables, update it today.

Update every Custom Tables site to 3.7.8

Treat every version from 1.0 to 3.7.7 as affected. The upload needs no login, only a public submission form with a file field, and the file is written to Joomla's own temp folder, which on a default install sits inside the web root. Update the whole Custom Tables package, not just the component, then check the temp folder for files you did not put there.

9.5
CVSS 4.0

CVE-2026-105606 Unauthenticated arbitrary file upload in Custom Tables

CRITICAL Joomla CNA

Any visitor can write a file with an extension of their choosing into the web-accessible temp folder of a Joomla site that exposes a public Custom Tables submission form, and host attacker-controlled content, such as phishing or malware pages, under the site's domain.

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

No login needed | Needs a public submission form with a file field | Versions 1.0 to 3.7.7

▼ 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:H` High: Data and files can be altered at will
`VA:H` High: The site can be taken down

What it does beyond the site

`SC:H` High: Data on other systems can be read
`SI:H` High: Other systems can be altered
`SA:H` High: Other systems can be taken down

How the Custom Tables upload flaw works

Custom Tables lets a Joomla site build its own data tables and put a submission form for them on the public side of the site, and a field on that form can accept a file. In 3.7.7 and earlier, the front-end uploader behind that field, `site/libraries/customtables/helpers/FileUploader.php`, made two decisions that did not belong together. It took the file extension from the file name the browser sent, which the sender controls, and it judged whether the upload was acceptable only by the MIME type PHP detected from the file's content.

That gap is what a polyglot exploits. A polyglot is a file whose content reads as one type, say an image, while also containing something else, so the content check passes and the file is saved under whatever extension the sender named. The uploader moved it into Joomla's temp folder as `ct_<timestamp>_<field id>_<original filename>`, and the JSON response returned that file name, so the attacker knew the path without guessing.

The temp folder is Joomla's own `tmp_path`, the value shown in Global Configuration under Server as Path to Temp Folder. On a default install that is the `tmp` folder in the site root, inside the web root, so a file written there can be fetched from the site's domain. According to the CVE record, the file is served as static content by default, so the stated impact is an unauthenticated file write to a web-accessible folder, which lets an attacker host their own content, phishing or malware pages for example, under the victim's domain. The weakness class is CWE-434, unrestricted upload of a file with a dangerous type.

The CVSS vector reads AT:P, attack requirements present, because the attacker needs a public Custom Tables submission form with a file field to exist on the site. Where it does, nothing else stands in the way: no login, no user interaction.

What Custom Tables 3.7.8 changes

The fix is public, because Custom Tables is open source. It is two commits in the GitHub repository, both titled "Arbitrary File Upload via Content-MIME/Extension Mismatch in Custom Tables File Uploader": f6eff3cefc on 13 October 2026 and 631248550e on 21 October 2026. Between them, the uploader in 3.7.8:

- rejects any extension on a blocklist of server-side script and server config types, including php, php3 to php8, phtml, pht, phar, phps, shtml, cgi, pl, py, asp, aspx, jsp, htaccess and htpasswd;
- requires the extension to be on the field's own allowed list, instead of accepting anything whose content passed the MIME check;
- reads the extension with `pathinfo()` instead of splitting the name on dots;
- rejects the record on save with "File extension mismatch", and deletes the file, when the stored extension differs from the destination name.

The same release closes a second flaw: an authenticated path traversal through an unvalidated file-field value that allowed arbitrary file deletion, tracked as GitHub advisory GHSA-rphh-5v5h-qv35 and fixed in commit 546a0cf3c1 on 21 October 2026. We have seen no CVE for that one. Updating to 3.7.8 covers both.

A third of Custom Tables sites have updated

Custom Tables 3.7.8 first appeared on a Joomla site connected to mySites.guru on 21 October 2026, the day of the second fix commit. The CVE followed twelve days later, on 2 November.

On 2 November, across the connected Joomla sites running the Custom Tables component, about a third are on 3.7.8. About two thirds are still on an affected version, every one of them between 3.6.5 and 3.7.7, so these are not forgotten installs on ancient builds; they are sites that were kept close to current and then stopped twelve days short of the one update that mattered.

That is the usual shape of an extension fix. The commit title named the flaw on the day it was pushed, yet without a CVE or a vendor notice to point at it, a 3.7.8 release looks like any other minor update, and site owners who update on a schedule rather than on a signal had no reason to move it up the queue. The CVE gives them that signal.

How mySites.guru flags Custom Tables below 3.7.8

mySites.guru records the installed extensions and their versions on each connected Joomla site twice a day, and flags any site running a version listed in its Joomla vulnerability database on the site's own card and in its audit. The rule for CVE-2026-105606 went live on 2 November 2026, and connected sites running `com_customtables` below 3.7.8 are flagged, with 3.7.8 shown as the version that resolves it. The CVE-2026-105606 page has the record.

The flag watches the component, because that is where the upload code lives. The Custom Tables name covers more than the component, though: a content plugin, a Web Services plugin, a task plugin, modules for Add Record, Catalog and ChatGPT, and a Custom Tables Pro Package. Update the whole package to 3.7.8, so the companions stay in step with the component they depend on.

Not our finding

The CVE record credits Valentin Lobstein (Chocapikk) as the finder. We did not find this flaw; we cover it because sites we monitor run the extension. He also found the JCTables SQL injection, CVE-2026-76570, that we wrote up in September, and he is one of several researchers auditing the same Joomla extensions we are. We found no technical write-up from him for Custom Tables at the time of writing, so the detail above comes from the CVE record and the 3.7.8 code.

CVE-2026-105606 is not on CISA's Known Exploited Vulnerabilities list as of 2 November 2026. It sits in a long run of Joomla extension security issues this year, and like most of them the fix was public before the record.

What to do on every Joomla site running Custom Tables

1. Take a backup, then update the whole Custom Tables package to 3.7.8. Afterwards, check that any public submission forms and their file fields still work.
2. If a site cannot be updated at once, unpublish or restrict the menu items and modules that show a public Custom Tables add or edit form. That removes the entry point until the update is in.
3. Look in the temp folder, the Path to Temp Folder under Global Configuration, Server, for files whose names start with `ct_` that you did not expect. Pay particular attention to script files, `.htaccess` files and HTML pages. The vendor's new blocklist is of server-side script and server config types for a reason: if a script file is already sitting there and you did not put it there, treat the site as hacked.
4. Consider moving the temp folder outside the web root. That removes the "served from your domain" half of this flaw, and of the next one like it, though it is no substitute for the update. We covered the same folder in the JoomGallery unauthenticated upload post.
5. Look for recently modified PHP files across the whole site, not just the temp folder.
6. If you find planted files, start with the Joomla hacked-site guide.



Find files that match known hacks

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

Catch the next Joomla extension fix across every site

A release like this one is a list-building problem before it is an update problem: which of your sites run Custom Tables, on which version, and which of those show a public form with a file field. By hand that is a login per site. On mySites.guru the subscription answers the first two from the twice-daily snapshot, and every connected site running an affected version is flagged the day a rule goes in, with the version that resolves it.

The follow-up runs on the same subscription. The Joomla malware scanner looks for code planted on the server once someone has a way in, and the hacked files check above matches files against known hacks. If a site already looks hacked and you would rather hand it over, have us clean it for you.

If you manage Joomla sites for clients, see what the subscription costs, or run the free audit to see what it finds on your own sites first.

Further Reading

- CVE-2026-105606 on cve.org - the Joomla CNA record with the affected range, vector and credit.
- Custom Tables on GitHub - the open source repository where the 3.7.8 fix commits live.

- The second fix commit, 631248550e - titled Arbitrary File Upload via Content-MIME/Extension Mismatch in Custom Tables File Uploader.
- JoomlaBoat - the vendor of Custom Tables.
- CWE-434: Unrestricted Upload of File with Dangerous Type - MITRE's definition of the weakness class.
- JCTables SQL injection - our post on CVE-2026-76570, found by the same researcher.

Frequently Asked Questions

What is CVE-2026-105606?

An unauthenticated arbitrary file upload in Custom Tables, the Joomla extension by JoomlaBoat. The Joomla CNA published it on 2 November 2026 with a CVSS 4.0 score of 9.5 Critical. Versions 1.0 to 3.7.7 are affected, and 3.7.8 is the fix.

Which Joomla sites are exposed to the Custom Tables upload flaw?

Any site running Custom Tables below 3.7.8 that shows a public submission form with a file field. The attacker needs no login and no account; the form is the entry point. A site that only uses Custom Tables in the administrator area, with no public form, does not expose the vulnerable uploader to visitors.

Does the Custom Tables flaw let an attacker run code on my server?

The CNA says the uploaded file is served as static content by default, so the stated impact is hosting attacker-controlled content, such as phishing or malware pages, under your domain. The 3.7.8 fix adds a blocklist of server-side script and server config extensions, so treat any script file in your temp folder that you did not put there as a sign the site is hacked.

Which Custom Tables package do I update?

The upload code lives in the component, com_customtables, but the vendor also releases companion extensions under the same name: a content plugin, a Web Services plugin, a task plugin, Add Record, Catalog and ChatGPT modules, and the Custom Tables Pro Package. Update the whole package to 3.7.8 rather than the component on its own.

Where is the Joomla temp folder the files are written to?

Custom Tables uses Joomla's own tmp_path, shown in Global Configuration under Server as Path to Temp Folder. On a default install it is the tmp folder in the site root, which is why an uploaded file can be fetched from your domain. Moving that folder outside the web root stops the file being served, though it does not fix the upload itself.



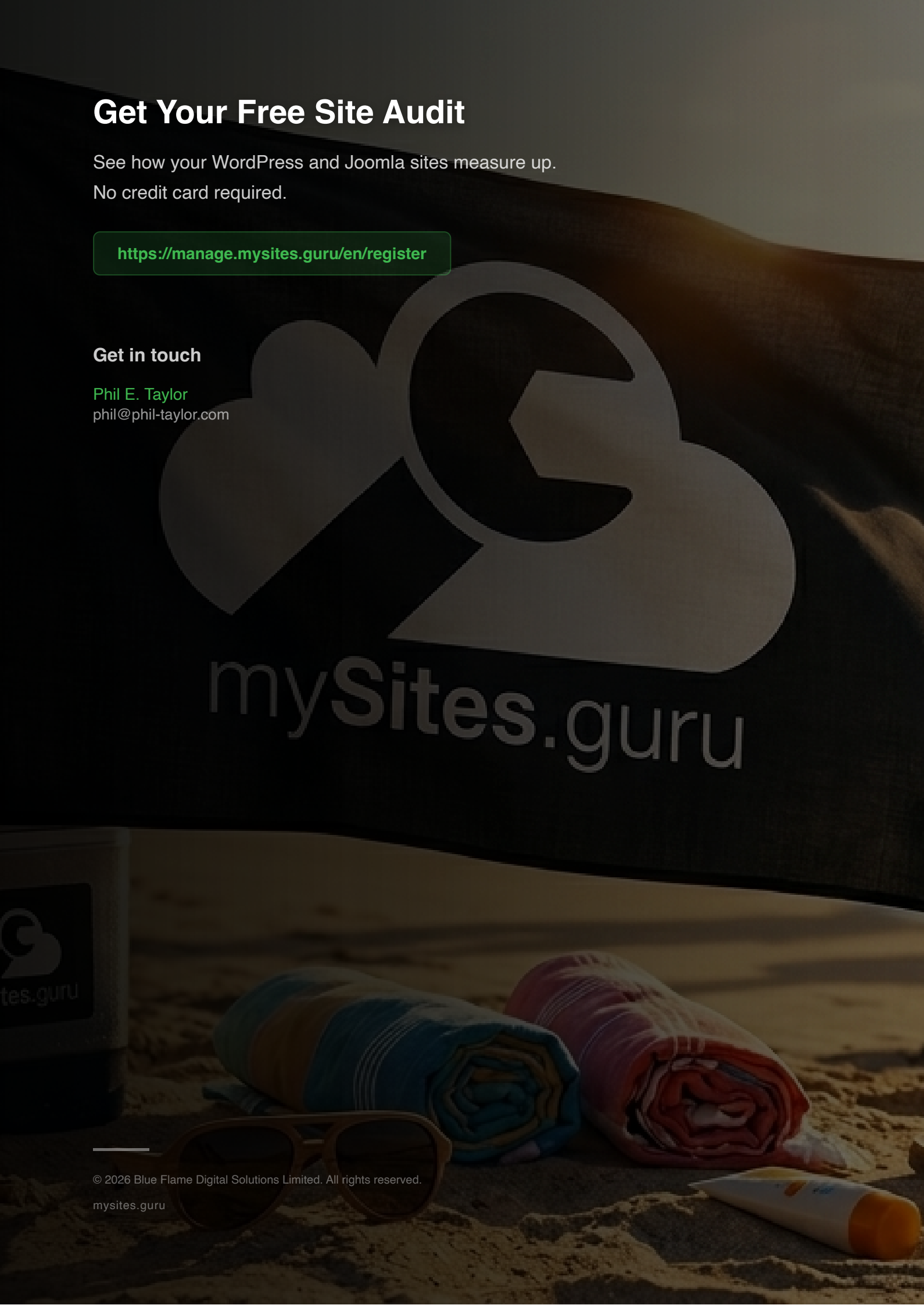
Written and edited by a human, with AI assistance. Our approach to AI

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.