



Articles Anywhere 20.1.1 and Sourcerer 17.0.1 Fix One Issue Together

CVE-2026-102802 is one Joomla extension fix split across Articles Anywhere 20.1.1 and Sourcerer 17.0.1: update both. Users Anywhere 3.0.1 fixes CVE-2026-102801.

Phil E. Taylor | 31 October 2026

Regular Labs released eight Joomla extension updates on 31 October 2026, and two of them have a **[SECURITY FIX]** entry with a CVE id. The one that matters most is CVE-2026-102802, fixed jointly in Articles Anywhere 20.1.1 and Sourcerer 17.0.1: before it, PHP in an article pulled into a trusted article through an Articles Anywhere tag ran on the server as if the trusted author had written it. The second, CVE-2026-102801 in Users Anywhere 3.0.1, stops a user tag from printing usernames and email addresses an administrator has switched off.

These are Joomla extension fixes, not Joomla core. The Articles Anywhere and Sourcerer entries each say the fix requires an updated copy of the other, so a site that updates only one of them is still exposed. Regular Labs found and fixed both issues itself and credits no one; we did not report them, and the CVE records are still reserved, so there is no official score or affected range yet.

What to do now

Update Articles Anywhere to 20.1.1 and Sourcerer to 17.0.1 on every Joomla 4, 5 and 6 site that runs both, Free or Pro. Updating one without the other does not close CVE-2026-102802. Update Users Anywhere to 3.0.1 wherever it is installed.

7.7
CVSS 4.0

CVE-2026-102802 Articles Anywhere and Sourcerer: PHP in an included article runs under the including article's trust

HIGH

mySites.guru (provisional: the CVE record is not yet published)

A content author whose articles are not trusted to run Sourcerer PHP could have PHP they wrote executed on the server, if a trusted article included their article through an Articles Anywhere tag. Running PHP on the server means doing anything the site's PHP can do. A site without Sourcerer is not affected.

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

Content author account needed

Free and Pro

Needs Sourcerer installed

▼ 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:L Low: Any logged-in account will do

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:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

5.3

CVSS 4.0

CVE-2026-102801 Users Anywhere: user tags override disabled username and email output

MEDIUM

mySites.guru (provisional: the CVE record is not yet published)

An administrator can switch off username and email output in the Users Anywhere settings. Before 3.0.1 a tag in an article could override that, so a content author could print the usernames and email addresses of site users on a public page.

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

Content author account needed

Free and Pro

▼ 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:N None: Works against any affected install

PR:L Low: Any logged-in account will do

UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:L Low: Some data 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

TL;DR

- **Articles Anywhere 20.1.1 and Sourcerer 17.0.1** together fix [CVE-2026-102802](#): PHP in an article included through Articles Anywhere ran under the including article's trust, so an untrusted content author's code could run on the server. Our provisional score is 7.7 High
- Each update needs the other. An old Articles Anywhere never tells Sourcerer about the included article, and an old Sourcerer never listens, so update both
- A site with Articles Anywhere and no Sourcerer is not exposed to this issue, but mySites.guru flags it anyway, because the flag tests one extension's version
- **Users Anywhere 3.0.1** fixes [CVE-2026-102801](#): user tags could override the settings that hide usernames and email addresses. Our provisional score is 5.3 Medium
- Both CVE ids are reserved, with no published record, score or range yet. Nothing is in CISA KEV and there is no report of exploitation in the wild
- On release day, 64% of the Articles Anywhere installs we monitor are on an affected build, and 44% of those also have Sourcerer installed

- Free and Pro share one version number, so every flag covers both editions. Joomla 3 gets no fix, because the Joomla 3 Sourcerer branch is frozen before any of the trust checks existed

Why Articles Anywhere and Sourcerer have to be updated together

Articles Anywhere inserts the content of another article into the article it is placed in. Sourcerer runs PHP that is written inside an article, and since 13.0.0 it decides whether to run it by who wrote the article: PHP runs only in content created and last modified by trusted users, Super Users by default, and 17.0.0 decides on the last editor, falling back to the creator. Each extension does its own job correctly; the gap was in how they work together.

Before the fix, Articles Anywhere pasted the included article's text into the host article, and Sourcerer then judged that text as part of the host article, under the host article's author. If the host was written by a Super User, everything inside it was trusted, including the paragraphs a content author had written in a different article and never had the rights to run PHP in.

Articles Anywhere 20.1.1 now passes each included article to Sourcerer first, through a new event (`onRegularLabsArticlesAnywherePrepareText`), together with that article's own creator and last editor. Sourcerer 17.0.1 listens for the event and applies the included article's own trust before the text reaches the host. That is why Regular Labs wrote "requires an updated Sourcerer" on one changelog and "requires an updated Articles Anywhere" on the other: an old Articles Anywhere never sends the event, and an old Sourcerer never listens for it.

The practical consequence is for sites where both extensions are installed and someone other than a Super User can write articles. A content author whose own articles are not trusted could get PHP they wrote executed on the server, provided a trusted article included theirs. An Articles Anywhere tag that selects articles by category rather than by a fixed id pulls in every new article in that category, so a new article from an untrusted author arrives inside the trusted one with no help from

anybody. Once PHP runs on the server, the author can do anything the site's PHP can do. A site without Sourcerer is not affected.

What a trusted article is in Sourcerer

Sourcerer 17.0.0 has trusted User Groups settings for PHP, and Regular Labs describes this fix in terms of "trusted" articles: an article is trusted when the people who created it and last edited it belong to those groups. The 13.0.0 release on 22 July 2026, the [CVE-2026-64796](#) fix, introduced that check, and 17.0.0 refined it to look at the last editor first.

The check was always applied to the article Sourcerer was looking at. The include path skipped it because, by the time Sourcerer looked, there was only one article to see: the host, with somebody else's text already inside it. 20.1.1 and 17.0.1 make sure the check sees each article on its own.

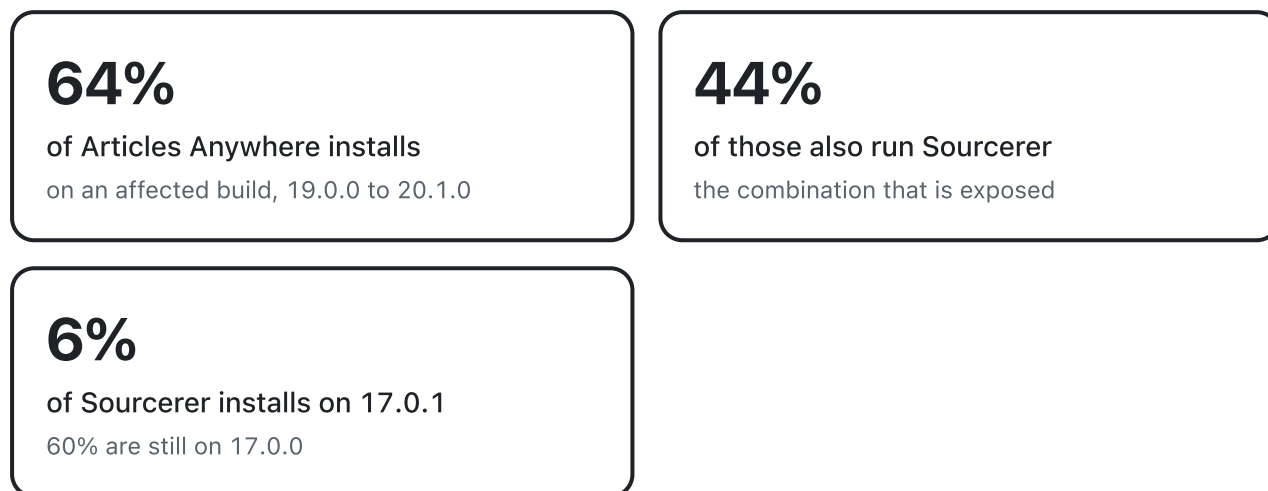
Users Anywhere 3.0.1 hides usernames and emails again

Users Anywhere shows user details inside content through tags. Administrators can switch off username and email output in the plugin settings.

Before 3.0.1, a user tag could override those settings. A content author could therefore write a tag that printed the usernames and email addresses of site users on a public page, regardless of what the administrator had disabled. The changelog entry reads "Prevents user tags from overriding disabled username and email output settings", and it is marked as a security fix with [CVE-2026-102801](#) for Free and Pro. Our provisional assessment is 5.3 Medium: it needs a content author account, and the outcome is disclosure rather than control.

How many Joomla sites are exposed on release day

Across the Joomla sites connected to mySites.guru, most Articles Anywhere installs were on an affected build on the day the fix was released, and a little under half of those also have Sourcerer installed, which is the combination this issue actually needs.



Share of installs on Joomla sites connected to mySites.guru, measured on 31 October 2026, release day.

Only 7% of Articles Anywhere installs had reached 20.1.1 by the time we measured. Users Anywhere is a much smaller install base, and nearly every Users Anywhere install we monitor is below 3.0.1.

This is the fifth Regular Labs security round we have covered since July. The [22 July catalogue-wide release](#) introduced the trusted-author check in Sourcerer; [Sourcerer then needed three releases in nine days](#) in August to close [CVE-2026-74253](#); the [13 September batch](#) updated 24 extensions with 10 security fixes; and on 27 September [Modules Anywhere 10.0.0 and Tabs & Accordions 3.2.0](#) closed two more content author holes. Many of these fixes are the same class of problem, content from a less-trusted user reaching a more-trusted context, closed one path at a time. This round closes the path through Articles Anywhere, and the next path may be a few weeks away.

The rest of the 31 October Regular Labs batch

Six of the eight releases have no security entry. Two are worth taking anyway.

Extension	Version	What changed	Security fix?
Articles Anywhere	20.1.1	Passes included articles to Sourcerer with their own trust (needs Sourcerer 17.0.1)	Yes, CVE-2026-102802
Sourcerer	17.0.1	Applies an included article's own trust (needs Articles Anywhere 20.1.1)	Yes, CVE-2026-102802
Users Anywhere	3.0.1	User tags can no longer override disabled username and email output	Yes, CVE-2026-102801
Cache Cleaner	10.1.0	* wildcards in Ignore Files/Folders; Pro: CDN provider requests now verify the TLS certificate	Not labelled, worth taking
ReReplacer	16.3.0	Pro: a PHP escape tag, and warnings about captured or visitor-supplied text in PHP replacements	Not labelled, worth taking
Snippets	11.1.1	Pro: Articles Anywhere values now override variables in trusted Snippets tags (needs an updated Articles Anywhere)	No
Articles Field	5.1.0	Functional fixes	No
Extension Manager	9.3.6	Functional fixes	No

The Cache Cleaner Pro change stops its CDN provider requests being sent without TLS certificate verification. Regular Labs did not label it a security fix and there is no CVE, but a CDN request without certificate checks can be intercepted, so take the update. The ReReplacer change is hardening rather than a fix: an escape tag and warnings for anyone who feeds captured or visitor-supplied text into a PHP replacement.

Joomla 3 sites

Articles Anywhere 20.x and Sourcerer 17.x run on Joomla 4, 5 and 6 only, with PHP 8.2 as the minimum. The Joomla 3 branch of Sourcerer is frozen at 9.8.0, which predates

13.0.0 and every trusted-author check that came with it. On Joomla 3, Sourcerer runs PHP from any article author already, included or not, so this particular issue is moot there because the earlier and broader one was never fixed on that branch. The [Regular Labs page on joomla3security.com](#) covers where Regular Labs stands on Joomla 3. If a Joomla 3 site runs Sourcerer and anyone other than a Super User can write articles, that is the problem to deal with.

How mySites.guru flags these Regular Labs releases

mySites.guru records the version of every extension on every connected Joomla site twice a day. Since 31 October it flags [Articles Anywhere 19.0.0 to below 20.1.1](#) for [CVE-2026-102802](#) and [Users Anywhere below 3.0.1](#) for [CVE-2026-102801](#), on the dashboard and in the audit of every site that matches, with the version that resolves it. Articles Anywhere builds below 19.0.0 were already flagged for earlier issues. Free and Pro share one version number, so each flag covers both editions.

The [CVE-2026-102802](#) flag is on Articles Anywhere, which has two consequences. A flag can only test one extension's version, not whether two extensions are installed together, so a site running Articles Anywhere without Sourcerer is flagged even though it is not exposed; updating Articles Anywhere is free and clears it. And Sourcerer 17.0.0 is not separately flagged for this issue, so a site that clears the Articles Anywhere flag and stops there has done half the job: update Sourcerer too. The [vulnerable extension list](#) explains how these flags work for every extension we track.

When eight extensions from one vendor move on the same day, the site-by-site update is the part that gets skipped. mySites.guru can [update Joomla extensions across every connected site](#) from one screen, and if you would rather not babysit the next Regular Labs wave, [enable extension auto-updates](#) for the extensions you trust.

Who can write articles on your Joomla sites?

[CVE-2026-102802](#) starts with an account that can write an article, and ends with PHP running on the server, so the size of the risk on a given site is the number of those

accounts and how carefully they were given out. On a brochure site where two staff members write content and both are Super Users, it is small. On a membership site, a school, a club, or anything that lets people register and contribute, the author role is exactly where an attacker would start.

Until every site has both updates:

- Check whether front-end registration is switched on, and whether a new user can reach a group with authoring rights
- Remove authoring rights from accounts that no longer need them, and delete accounts that have never logged in
- Find the Articles Anywhere tags that select articles by category or other criteria rather than by a fixed id, because those pull in new articles from anyone allowed to write in that category
- Review recently created articles that contain `{source}` tags if you do not trust every author on the site

Disable User Registration Unless Required

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 →

If you find PHP you did not put there, treat the site as compromised and work through [our Joomla hacked-site guide](#), or have us [fix it for you](#).

If you run Regular Labs extensions on more than a few sites, [mySites.guru](#) flags every connected site the day a Regular Labs fix is released, and the [free audit](#) shows what it finds on your own sites first.

Further Reading

- [Regular Labs latest releases](#) - the vendor's changelog index for the whole batch
- [Articles Anywhere changelog](#) - the 20.1.1 security entry
- [Sourcerer changelog](#) - the 17.0.1 security entry
- [Users Anywhere changelog](#) - the 3.0.1 security entry
- [CVE-2026-102802](#) - our record page for the Articles Anywhere and Sourcerer issue
- [CVE-2026-102801](#) - our record page for the Users Anywhere issue
- [Sourcerer 14 and 15 did not fix CVE-2026-74253. 16.0.0 does.](#) - the August Sourcerer round, three releases in nine days
- [Modules Anywhere 10.0.0 and Tabs & Accordions 3.2.0 Close Two Content Author Security Holes](#) - the previous Regular Labs security round

Frequently Asked Questions

What did Regular Labs fix in Articles Anywhere 20.1.1 and Sourcerer 17.0.1?

One issue, [CVE-2026-102802](#). Sourcerer only runs PHP in articles written by trusted users, but an article pulled into a trusted article through an Articles Anywhere tag was judged as part of the trusted article, so PHP written by an untrusted content author could run on the server. Articles Anywhere 20.1.1 now passes each included article to Sourcerer with its own author details, and Sourcerer 17.0.1 applies that article's own trust.

Do I need to update both Articles Anywhere and Sourcerer?

Yes, on any site that has both installed. An old Articles Anywhere never tells Sourcerer about included articles, and an old Sourcerer never listens, so updating only one of them leaves the issue open. Regular Labs says so in both changelogs: each fix requires the other.

My site has Articles Anywhere but not Sourcerer. Am I affected?

No. Without Sourcerer there is nothing to run PHP in an article, included or not. mySites.guru still flags Articles Anywhere below 20.1.1, because a flag tests one extension's version and cannot see whether Sourcerer is also installed. Updating Articles Anywhere is free and clears the flag.

Is there an official CVSS score for CVE-2026-102802?

Not yet. Both CVE ids are reserved and the Joomla CNA has not published the records, so there is no official score, weakness class or affected range. Our own provisional assessment is 7.7 High for [CVE-2026-102802](#) and 5.3 Medium for [CVE-2026-102801](#), and we will update the post when the records appear.

Do these fixes apply to the Free editions?

Yes. Neither security entry is marked Pro, so Free and Pro are both affected and both fixed. Regular Labs releases Free and Pro under one version number, so the same update applies to either edition.

Will updating Articles Anywhere, Sourcerer or Users Anywhere break anything?

The changelogs mark no breaking change for Articles Anywhere 20.1.1, Sourcerer 17.0.1 or Users Anywhere 3.0.1. All three are point releases. The one behaviour change is the intended one: PHP in an included article written by an untrusted author stops running.

AI MODIFIED

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

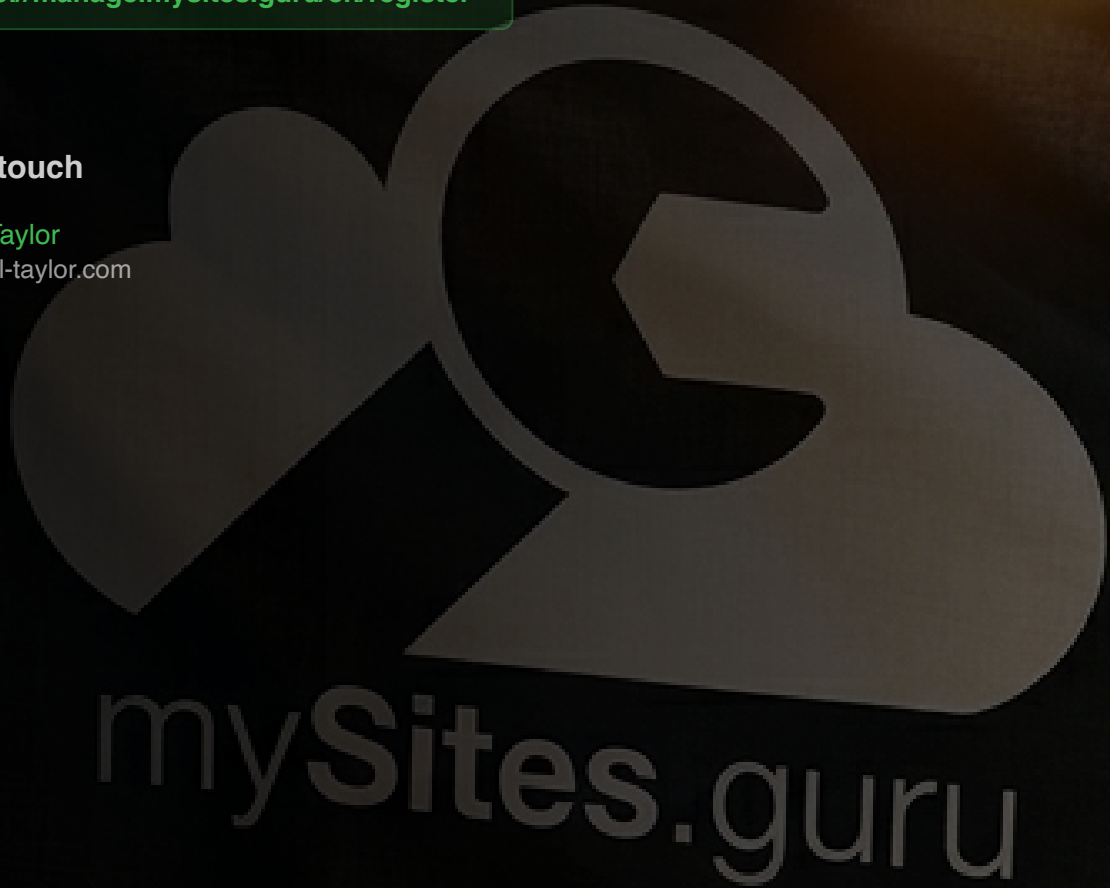
Get Your Free Site Audit

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