



iCagenda 4.0.17 Fixes a Stored XSS in Event Custom Fields

iCagenda 4.0.17 and PRO 3.9.17 fix a stored XSS in url-type event custom fields and a CSV formula injection in registration exports. Update every Joomla site.

Phil E. Taylor | 27 October 2026

JoomliC released **iCagenda 4.0.17** on 27 October 2026, labelled Security Release, alongside iCagenda PRO 3.9.17 for Joomla 3. iCagenda is a third-party Joomla extension, an events calendar, so this concerns only sites that have it installed. Both releases fix the same two issues. A url-type event custom field was printed into the page as a link with no escaping, so an event submitted from the site's front end could run JavaScript in the browser of whoever viewed it. And the registrations export did not neutralise spreadsheet formulas, so a value typed into the public registration form could run as a formula when an administrator opened the CSV.

The stored XSS affects iCagenda 3.2.1 through 4.0.16 and the CSV formula injection affects 3.5.0 through 4.0.16. The fix is 4.0.17 on Joomla 4, 5 and 6. On Joomla 3 it is iCagenda PRO 3.9.17, which needs a Pro subscription, because the free 3.9 line has reached end of life. Update now.

TL;DR

- **iCagenda 4.0.17** fixes a stored cross-site scripting flaw in url-type event custom fields (CVE-2026-102790, vendor severity High) affecting 3.2.1 through 4.0.16
- It also fixes a CSV formula injection in the registrations export (CVE-2026-102799, vendor severity Medium) affecting 3.5.0 through 4.0.16
- Both CVE ids are reserved and the records are not published yet, so there is no official CVSS score. Our provisional CVSS 4.0 assessments are 5.1 Medium and 2.1 Low. Neither is in the CISA Known Exploited Vulnerabilities catalog
- Reported to JoomliC by Akinlabi Omoogun of lulztigre.pw. Not a mySites.guru finding
- On Joomla 3 the only fixed release is **iCagenda PRO 3.9.17**, for Pro subscribers. Free 3.9 gets no more updates
- 4.0.17 is the fourth security release on the 4.x line since June
- mySites.guru flags every connected Joomla site on an affected version from the day of the release

5.1

CVSS 4.0

CVE-2026-102790: stored XSS via url-type event custom field

MEDIUM

mySites.guru provisional assessment (CVE record not published; Joomla! rates it High)

A user who can submit an event from the front end, Registered by default, can store JavaScript in a url-type custom field that runs in the browser of anyone who views that event, including site staff reviewing submissions.

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

Stored XSS

Registered user by default

Fixed in 4.0.17 and 3.9.17 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:P Passive: Someone has to visit a page

What it does to the site

VC:N None: Nothing can be read

VI:N None: Nothing can be altered

VA:N None: The site stays up

What it does beyond the site

SC:L Low: Some data on other systems can be read

SI:L Low: Some data on other systems can be altered

SA:N None: Other systems stay up

2.1

CVE-2026-102799: CSV formula injection in the registrations export

CVSS 4.0

LOW

mySites.guru provisional assessment (CVE record not published; Joomla! rates it Medium)

Anyone who registers for an event can type a value starting with a formula character, which runs when an administrator exports the registrations as CSV and opens the file in a spreadsheet application.

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

CSV injection

Needs an admin export

Fixed in 4.0.17 and 3.9.17 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:P Present: Needs a particular deployment or race to line up

PR:N None: No account needed

UI:A Active: Someone has to be talked through a few steps

What it does to the site

VC:N None: Nothing can be read

VI:N None: Nothing can be altered

VA:N None: The site stays up

What it does beyond the site

SC:L Low: Some data on other systems can be read

SI:L Low: Some data on other systems can be altered

SA:N None: Other systems stay up

What Joomla! fixed in iCagenda 4.0.17

The [4.0.17 changelog](#) and the [PRO 3.9.17 changelog](#) list the same two security entries, word for word:

- "Fixed: Stored XSS via url-type event Custom Field." This is CVE-2026-102790, which the vendor rates High.
- "Fixed: CSV formula injection in the registrations export." This is CVE-2026-102799, which the vendor rates Medium.

The vendor advisory gives each issue a probability as well as a severity: High for the XSS and Low for the CSV issue, with the note that "Vulnerability #2 is more limited in scope: the user has to export the file from Joomla administration and open it in a spreadsheet application." It credits Akinlabi Omoogun of lulztigre.pw with the report, and it makes no statement about exploitation in the wild. It also says "We deliberately choose not to publish functional proofs of concept," so the advisory does not describe how either flaw works.

One line in the advisory explains why an earlier review missed the XSS: "A previous review of the same code covered only the image, file and website fields, not event custom fields, so this sink had not been traced back then." The url custom field type has existed since iCagenda 3.6.0 in 2016. The vendor still lists 3.2.1 as the first affected version, and we follow the vendor on the range.

The stored XSS in iCagenda event custom fields

Someone who can submit an event from the site's front end could put JavaScript in a url-type custom field, and that JavaScript ran in the browser of whoever viewed the event. On a default install that someone is a Registered user: the submission form's access setting defaults to Registered, and it is open to anonymous visitors only where a site administrator set it to Public. That is why our provisional score marks privileges required as Low rather than None, and why it comes out at 5.1 Medium where the vendor says High. The vendor's rating is a fair one for a site that opened the form to the public.

Before 4.0.17, the shared iCagenda library function that turns a URL into a link printed the value straight into an `<a href="...">` tag and again as the link text, with no HTML escaping and no check on the link's scheme. A `javascript:` address, or a value that

broke out of the attribute, went into the page as written. 4.0.17 escapes both the attribute and the text, and only renders a link for http and https addresses; anything else is printed as plain escaped text.

The front-end submission form was tightened at the same time. It now keeps only values for custom fields that are published, and for url-type fields it rejects any value containing quotes, angle brackets, whitespace or control characters, or using a scheme other than http or https. A `javascript:` link is rejected at submission rather than stored and escaped later.

The people most likely to see a submitted event first are the site's own staff, because reviewing submissions means opening them. The script runs in the browser of whoever views the event, with whatever that visitor is logged in as on the front end.

The CSV formula injection in iCagenda registration exports

Registrations come from the public registration form, so whoever registers chooses the name, email, custom field values and notes. Before 4.0.17 the registrations export wrote those values into the CSV as typed, and a value starting with `=`, `+`, `-` or `@` is read by a spreadsheet application as a formula. The formula runs when an administrator opens the export.

4.0.17 prefixes an apostrophe to any free-text cell that starts with one of those characters, or with a tab or carriage return, so a spreadsheet treats it as text. That is applied to the event title, name, email, custom field values and notes.

The vendor rates this Medium with a Low probability, and our provisional CVSS 4.0 score is 2.1 Low: it needs an administrator to export the file and open it in a spreadsheet application. A CSV exported before the update is still the old file, which matters for the steps at the end of this post.

iCagenda PRO 3.9.17 and Joomla 3 sites

iCagenda 3.9 is the final version for Joomla 3, and the free 3.9 line reached end of life on 13 October 2026 with no more updates. Joomla!C extended security support for iCagenda PRO 3.9 only, until 13 October 2027, for Pro subscribers. So 3.9.17 is available only with a Pro subscription, and a Joomla 3 site running the free edition has no fixed release at all.

Both flaws affect the 3.x line: the XSS from 3.2.1 and the CSV injection from 3.5.0. A Joomla 3 site on free iCagenda 3.9.16 or earlier has three options. Buy a Pro subscription and install 3.9.17. Apply the vendor's interim mitigations, which are to disable the menu item that allows event submissions from the front end and to stop exporting registrations as CSV from the administrator, and accept that those are workarounds rather than a fix. Or move the site to Joomla 5 or 6 and install iCagenda 4.0.17. Joomla!C's own position is the third: "We strongly advise users who are still using Joomla! 3 to upgrade to Joomla! 5 and Joomla! 6 as soon as possible."

Joomla 3 reached end of life in August 2023, and iCagenda 4.x needs Joomla 4 at minimum, with Joomla 4.4 itself end of life since 17 October 2025. The [iCagenda page on joomla3security.com](#) sets out where the extension stands on Joomla 3, and the [stay, patch or migrate options](#) page covers the choice for the site as a whole. If you run Joomla 3 sites for clients, [what the end of life means for agency retainers](#) is the post to read next.

iCagenda sites on release day

Among the Joomla sites in the mySites.guru database that run iCagenda and took a snapshot in the 30 days to 27 October 2026:

87%

on an affected version

On release day, across both lines

28%

on the Joomla 3 line

iCagenda 3.x, where the only fix needs Pro

73%

42%

of 4.x sites on 4.0.16

One update away; 10% already on 4.0.17

of 3.x sites below 3.9.15

Still open to the June file upload RCE in the CISA KEV catalog

Joomla sites running iCagenda with a snapshot in the 30 days to 27 October 2026, mySites.guru database. Percentages of those sites, or of the named subset.

The 4.x line looks healthy. 73% of those sites are on 4.0.16, so they installed the previous release and are one update from current, and 10% had 4.0.17 on the day it came out. Only 4% are still below 4.0.12, which leaves them open to the [August SQL injection in the Calendar module](#) as well.

The Joomla 3 line splits in two. 19% of the 3.x sites were already on 3.9.17 on release day, which means they hold a Pro subscription and update fast. 39% are on 3.9.15 or 3.9.16. The remaining 42% are below 3.9.15, so they have not updated since before June and still have the [unauthenticated file upload to RCE](#) that is listed in the CISA Known Exploited Vulnerabilities catalog. Those sites need more than 3.9.17.

Which of your Joomla sites need iCagenda 4.0.17?

mySites.guru records the installed version of every extension on every connected Joomla site twice a day. Two rules went live on release day, one for iCagenda 4.0.0 to 4.0.16 and one for 3.2.1 to 3.9.16, so each connected Joomla site on an affected version is flagged on its dashboard and in its audit. The [iCagenda page of our vulnerability list](#) shows all of them together, with the June and August flaws beside these two.

From there, [update the flagged sites from one dashboard](#) rather than logging into each administrator in turn, or switch on [automatic extension updates](#) so the next iCagenda release installs itself. Four security releases on the 4.x line since June (4.0.8, 4.0.12, 4.0.13 and 4.0.17) is a good argument for that setting. The [vulnerable extension list](#) puts iCagenda alongside the other flagged extensions on your sites.

What to do now on Joomla sites running iCagenda

1. On Joomla 4, 5 or 6, [download](#) and install iCagenda 4.0.17.
2. On Joomla 3 with a Pro subscription, install iCagenda PRO 3.9.17.
3. On Joomla 3 without Pro, either buy Pro for 3.9.17, apply the vendor mitigations (disable the front-end event submission menu item and stop exporting registrations as CSV until you can update), or move the site to Joomla 5 or 6 with iCagenda 4.0.17.
4. After updating, review events submitted from the front end for odd values in url-type custom fields. Anything that is not a plain http or https address is suspect.
5. Treat any old registrations export with care. Do not open a CSV exported before the update in a spreadsheet; re-export it after updating.

If you look after more than a handful of Joomla sites, the gap between the sites that had 3.9.17 on release day and the 42% still below 3.9.15 is what happens when no one is checking the installed versions. [See what mySites.guru costs](#) for the number of sites you manage.

Further Reading

- [iCagenda security update, version 4.0.17](#) - Joomla!C's announcement, with the vendor severities, probabilities and interim mitigations
- [iCagenda 4.0.17 changelog](#) - the release notes for the Joomla 4, 5 and 6 line
- [iCagenda PRO 3.9.17 changelog](#) - the release notes for the Joomla 3 line, Pro subscribers only
- [iCagenda on joomla3security.com](#) - where iCagenda stands on Joomla 3 support, and what that means for a site still on it
- [Unauthenticated File Upload to RCE in iCagenda](#) - the June flaw we reported, fixed in 4.0.8 and 3.9.15, and listed in the CISA KEV catalog
- [Unauthenticated SQL Injection in the iCagenda Calendar Module](#) - the August flaw, CVSS 4.0 9.2 Critical, fixed in 4.0.12

Frequently Asked Questions

Is iCagenda 4.0.17 a security release?

Yes. Joomla!C labels both iCagenda 4.0.17 and iCagenda PRO 3.9.17 as Security Release. Each fixes the same two issues: a stored cross-site scripting flaw in url-type event custom fields and a CSV formula injection in the registrations export.

Which iCagenda versions are affected?

Per the vendor advisory, the stored XSS affects iCagenda 3.2.1 through 4.0.16 and the CSV formula injection affects 3.5.0 through 4.0.16. The fix is 4.0.17 on Joomla 4, 5 and 6, or iCagenda PRO 3.9.17 on Joomla 3.

Do the iCagenda 4.0.17 flaws have CVE ids?

Yes, CVE-2026-102790 for the stored XSS and CVE-2026-102799 for the CSV formula injection. Both ids are reserved and the records are not published yet, so there is no official CVSS score, CWE or affected range from a CVE record. Neither is in the CISA Known Exploited Vulnerabilities catalog.

Who can exploit the iCagenda stored XSS?

Anyone who can submit an event from the site's front end. The submission form's access setting defaults to Registered users, so on most sites that means someone with an account. It is open to anonymous visitors only where a site administrator set it to Public.

Is there a fix for iCagenda on Joomla 3 without a Pro subscription?

No. Free iCagenda 3.9 reached end of life on 13 October 2026 and gets no more updates. iCagenda PRO 3.9.17 is the only fixed release for Joomla 3, and it needs a Pro subscription. The alternatives are the vendor's mitigations or moving the site to Joomla 5 or 6 with iCagenda 4.0.17.

Does mySites.guru flag iCagenda below 4.0.17?

Yes. Two rules went live on release day for iCagenda 4.0.0 to 4.0.16 and 3.2.1 to 3.9.16, so every connected Joomla site on an affected version is flagged on its dashboard and in its audit.

AI MODIFIED

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

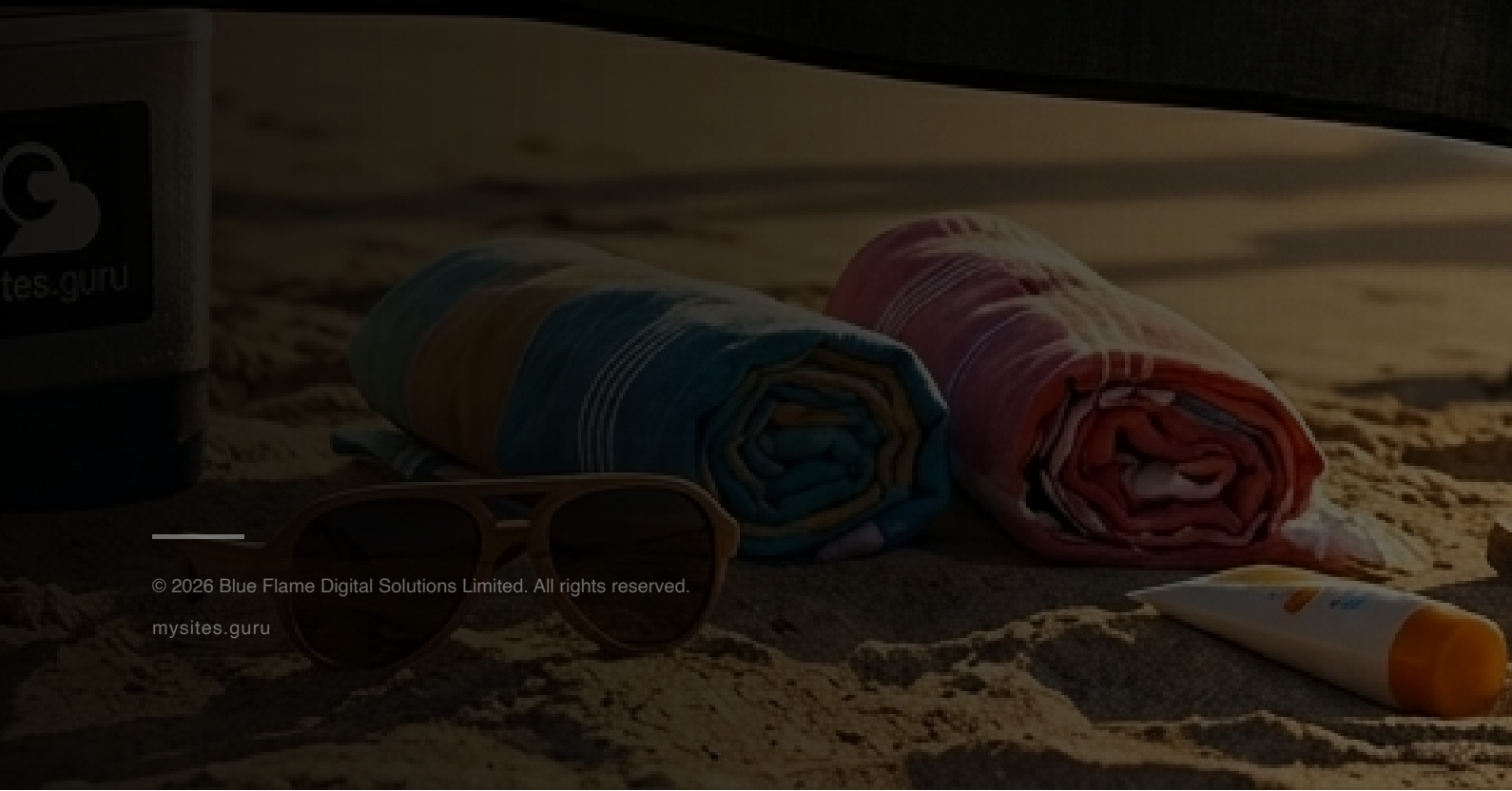
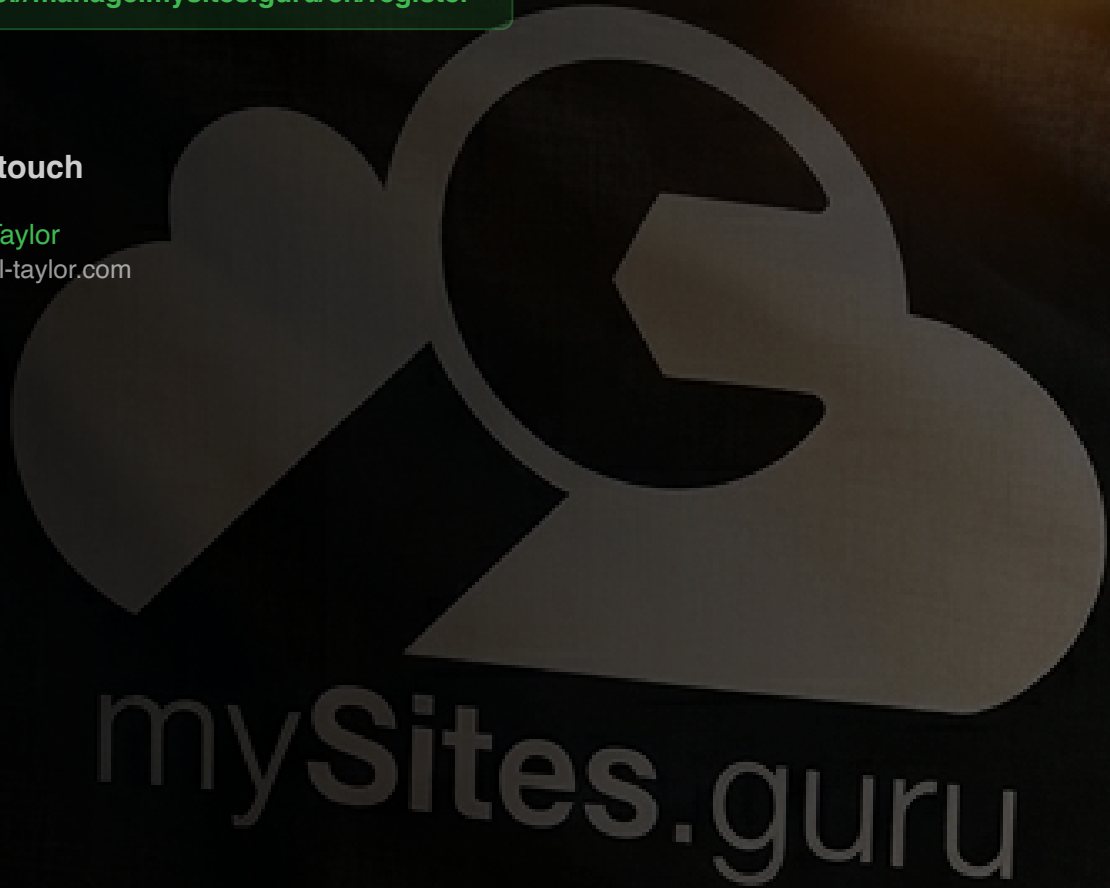
Get Your Free Site Audit

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