mySites.guru

iCagenda 4.0.12 fixes an unauthenticated SQL injection

CVE-2026-67365 is an unauthenticated SQL injection in the iCagenda Calendar module for Joomla, scored 9.2 Critical. Fixed in 4.0.12.

Phil E. Taylor | 17 August 2026

The Joomla project's CVE Numbering Authority published CVE-2026-67365 on 14 August 2026: an unauthenticated SQL injection in the iCagenda Calendar module, part of the iCagenda events extension for Joomla. It is scored **9.2 Critical** under CVSS 4.0, and the fix is **iCagenda 4.0.12**.

This is not our find. The CVE credits Joep van Antwerpen of Onvio. We found the previous iCagenda flaw in June, an unauthenticated file upload that ended up in the CISA Known Exploited Vulnerabilities catalog, so this is the second security issue in the extension in two months and the two are unrelated.

TL;DR

- **CVE-2026-67365**, published 14 August 2026 by the Joomla CNA, **CVSS 4.0 9.2 Critical**, CWE-89
- **Unauthenticated SQL injection** in the iCagenda Calendar module (`mod_icagenda_calendar`), described in the record as reachable **via** `com_ajax` **with no session, token or account**
- **Affected: 4.0.0 to 4.0.11. Fixed: 4.0.12**
- **The module version does not match the package version.** The Calendar module stayed at **4.0.7** through the 4.0.8, 4.0.9, 4.0.10 and 4.0.11 releases and only moved with 4.0.12, so a site can show iCagenda 4.0.11 while the vulnerable module reports 4.0.7

- **Reported by Joep van Antwerpen of Onvio**, not by us
- **No vendor release note.** The icagenda.com changelog lists nothing above 4.0.11 at the time of writing
- Separate from **CVE-2026-48939**, the file upload fixed in 4.0.8 and 3.9.15. Patched for that one does not mean patched for this one

What CVE-2026-67365 is

The CVE record is the whole public description, so here it is verbatim:

CVE-2026-67365, DESCRIPTION IN FULL

```
Joomla Extension – icagenda.com – Unauthenticated SQL
injection in iCagenda < 4.0.0–4.0.11 – Unauthenticated SQL
injection in mod_icagenda_calendar (iCagenda), reachable via
com_ajax with no session, token or account.
```

Three things in that sentence decide how quickly you act. It is **unauthenticated**, so nobody needs an account. It is reached through `com_ajax`, Joomla's generic front-end AJAX entry point, which is available to anonymous visitors by default and which we have written about before as a recurring blind spot. And it is **SQL injection**, so what is at risk is the contents of the database, which on a Joomla site includes the user table and its password hashes.

We have not written an exploit for this and we are not publishing one. Nothing here needs it.

The version number that will mislead you

This is the part worth your attention if you manage more than a couple of sites, and it is why a sensible-looking version check gives the wrong answer.

The vulnerable code is in a module, not the component, and **the module's version did not move with the package**. Across the Joomla sites we manage, the iCagenda Calendar module reports only a handful of distinct versions, and the pattern is clear: it sat at **4.0.7** while the package went through 4.0.8, 4.0.9, 4.0.10 and 4.0.11, then jumped straight to **4.0.12** when this fix shipped.

So on a site running iCagenda 4.0.11, the extension manager shows you 4.0.11 for the component and 4.0.7 for the Calendar module. Both are accurate. Neither, on its own, tells you whether this flaw is closed. The reading that does is the module at 4.0.12.

Two practical consequences:

- **A version comparison against the package version is wrong in both directions.** Written one way it misses affected sites, written another it flags patched ones. Our own rule matches the module and treats anything below 4.0.12 as affected, which is the only form that lines up with reality.
- **Sites without the Calendar module installed are not exposed through this route**, because the flaw is reached through that module. The component alone is not enough.

One open question we are not going to answer by guessing. iCagenda also ships an older calendar module, `mod_iccalendar`, labelled "deprecated", and it is still installed on plenty of sites. The CVE names `mod_icagenda_calendar` and only that, so we have not flagged the deprecated one as affected: doing so would mean asserting something the record does not say. If you still run `mod_iccalendar`, the safe assumption is that a deprecated module is not getting security attention either way, and the right move is to replace it rather than wait to find out.

Which Joomla sites are affected?

Any site with the iCagenda Calendar module below 4.0.12. The module is common but not universal on iCagenda sites: across the Joomla sites we manage, a bit under three quarters of iCagenda installs have the Calendar module, and more than four in ten of those are still on the vulnerable 4.0.7 today.

What to do

Update the iCagenda package to **4.0.12** or later, then confirm the **module** shows 4.0.12 rather than trusting the component version or the “up to date” message.

If you cannot update immediately, unpublishing and uninstalling the iCagenda Calendar module removes this exposure, because the flaw is reached through that module. That obviously removes the calendar from the site too, so treat it as a stop-gap.

One more thing worth doing on any site that has been sitting on an old iCagenda for a while: this extension had an actively exploited flaw two months ago, so it is worth checking the **Hacked?** section on each affected site and reading through **Users** in the Joomla admin for administrator accounts nobody created. Updating closes the door and tells you nothing about whether anyone already came through it.

Disclosure and severity

This flaw is CWE-89, SQL injection, reached over the network by an anonymous visitor with no privileges and no user interaction. Unlike our own assessments on vendor-silent releases, the numbers here are **official**: the Joomla CNA published a CVSS 4.0 vector with the record.

9.2
CVSS 4.0

CRITICAL **Official vector, published by the Joomla CNA**

Unauthenticated SQL injection reachable through com_ajax with no session, token or account. High confidentiality impact on the vulnerable component and a high impact on the wider system, which is what carries the score to Critical.

No login needed | Exploitable over the internet | No user interaction | Database read

Field	Detail
CVE	CVE-2026-67365, published 14 August 2026 by the Joomla CNA

Field	Detail
Component	iCagenda Calendar module (`mod_icagenda_calendar`) for Joomla, shipped with the iCagenda events extension
Vendor	JoomliC (icagenda.com)
Type	Unauthenticated SQL injection (CWE-89), reachable via `com_ajax`
CVSS 4.0	9.2 (Critical), `AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:H/SI:H/SA:H` (official, from the CVE record)
Affected versions	4.0.0 up to and including 4.0.11
Fixed in	4.0.12
Finder	Joep van Antwerpen, Onvio. Not a mySites.guru find
Vendor advisory	None. The icagenda.com changelog lists nothing above 4.0.11 at the time of writing

Further Reading

- CVE-2026-67365 at cve.org
- CWE-89: SQL Injection at MITRE
- iCagenda changelog at icagenda.com
- The iCagenda file upload we found in June, now in the CISA KEV catalog
- Why AJAX endpoints keep turning up in CMS advisories

Frequently Asked Questions

What is CVE-2026-67365?

An unauthenticated SQL injection in the iCagenda Calendar module (mod_icagenda_calendar), a module that ships with the iCagenda events extension for Joomla. The Joomla CNA published the record on 14 August 2026 and describes the flaw as reachable via com_ajax with no session, token or account. It is scored CVSS 4.0 9.2 Critical under CWE-89. The affected range is 4.0.0 to 4.0.11, and 4.0.12 is the first release that is not affected.

Which iCagenda versions are affected?

4.0.0 up to and including 4.0.11, per the CVE record. Update the iCagenda package to 4.0.12 or later. Note that this is a separate flaw from the arbitrary file upload we found in June 2026, CVE-2026-48939, which was fixed in 4.0.8 and 3.9.15 and is listed in the CISA Known Exploited Vulnerabilities catalog. Being patched against that one does not cover you for this one.

Why does my site show iCagenda 4.0.11 but the module says 4.0.7?

Because the module manifest version did not move with the package. The iCagenda Calendar module stayed at 4.0.7 through the 4.0.8, 4.0.9, 4.0.10 and 4.0.11 releases and only changed to 4.0.12. So a site can list iCagenda 4.0.11 in its extension manager while the vulnerable module still reports 4.0.7. Both numbers are correct and neither is the whole story. The one that tells you whether the flaw is closed is the module reading 4.0.12.

Who found this one?

Joep van Antwerpen of Onvio, credited in the CVE record. This is not a mySites.guru find. We found the previous iCagenda flaw, the unauthenticated file upload in June 2026, but this SQL injection was reported by someone else.

Did the vendor publish a release note for the fix?

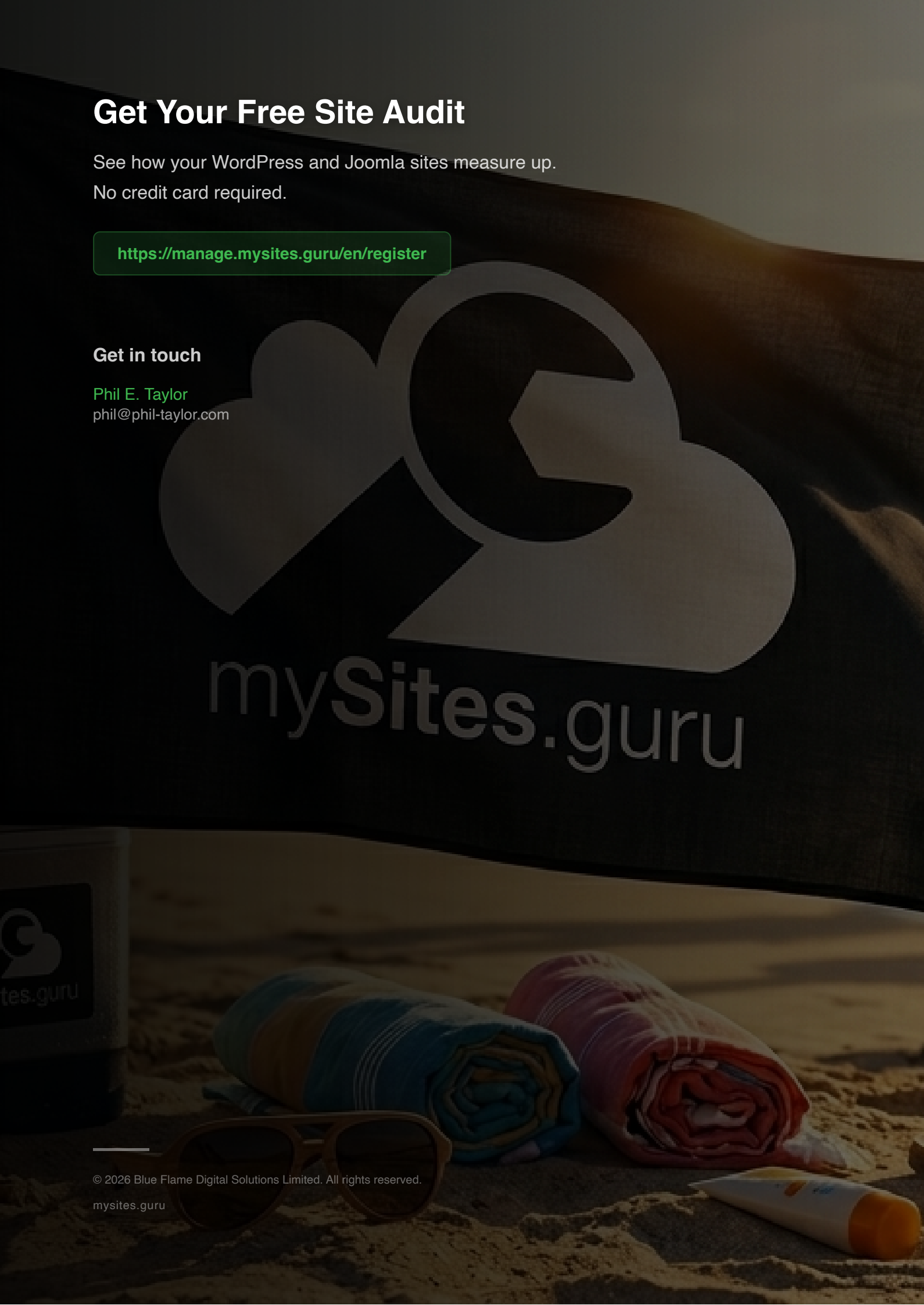
Not at the time of writing. The changelog at icagenda.com lists entries up to iCagenda 4.0.11, dated 18 July 2026, and nothing above it, even though 4.0.12 is shipping and installing on real sites. The CVE record is the public description of what changed.

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