YouTube Gallery for Joomla: Unauthenticated SQL Injection Fixed in 5.7.3

CVE-2026-94130: an unauthenticated SQL injection in JoomlaBoat's YouTube Gallery for Joomla, scored 9.3 Critical. Every version below 5.7.3 is affected.

Phil E. Taylor | 26 September 2026

TL;DR

CVE-2026-94130 is an unauthenticated SQL injection in YouTube Gallery, JoomlaBoat's video gallery extension for Joomla. The Joomla CNA published it on 26 September 2026 and scored it 9.3 Critical. Every version from 1.0.0 to 5.7.2 is affected, and the fix is 5.7.3.

No login is needed. The flaw sits in the public video search and in the router that maps friendly video URLs to database rows, so anyone who can load a page with a gallery on it can reach it. Update to 5.7.3. If you are on one of the old 4.x builds, there is no 4.x patch: 5.7.3 is the fix for you too.

9.3
CVSS 4.0

CVE-2026-94130 Unauthenticated SQL injection in video search and routing

CRITICAL Joomla CNA

Any visitor can inject SQL into the queries behind YouTube Gallery's front-end search and video URLs, and read data from the Joomla database.

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

No login needed | Public front end | Versions 1.0.0 to 5.7.2

▼ 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: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:N None: Other systems keep their data
SI:N None: Other systems keep their integrity
SA:N None: Other systems stay up

What went wrong in YouTube Gallery's queries

The CVE describes an injection in "video search functionality and sorting" that lets an attacker inject SQL into read queries. The two fix commits in JoomlaBoat's public repository show where. Both are cases of request input being pasted into a query string between quote marks, rather than being escaped or bound.

The search builds a `WHERE` clause from the `ygsearchquery` request parameter. Before 5.7.3 it wrapped each search term in double quotes after deleting any double quotes the visitor had typed. Stripping one character is not escaping, and SQL has more than one way to break out of a string. The 5.7.3 fix passes each term through Joomla's `$db->quote()` and each column name through `$db->quoteName()` against an allowlist, which is the correct pattern.

The router made the simpler version of the same mistake. Its fix is two lines:

```
// Before: the alias from the URL is concatenated straight into the query
$db->setQuery('SELECT videoid FROM #__youtubegallery_videos WHERE alias='

// After (5.7.3): the value is quoted and escaped by the database driver
$db->setQuery('SELECT videoid FROM #__youtubegallery_videos WHERE alias='
```

A router runs on every request that uses a search-engine-friendly URL for the component, which is about as public as a Joomla code path gets. It is the same class of problem we keep finding in front-end endpoints across Joomla extensions: code written on the assumption that only the extension itself will ever call it.

A malicious actor could extract your whole database: usernames, emails, password hashes, session IDs, shopping orders, invoices, and everything else it holds. Gulp.

If a vulnerable version was live on a site, our guide to checking Joomla database security covers what to review afterwards.

The fix was public two months before the CVE

JoomlaBoat committed the search fix on 26 July 2026 and the router fix on 27 July, both with commit messages that say “Security: Fixed SQL injection vulnerability”. The repository is public. Anyone watching it, or diffing 5.7.2 against 5.7.3, had a map of the vulnerable code from late July. The CVE, which is what most scanners and most site owners react to, arrived on 26 September.

There is one wrinkle in that history. The search fix bumped the version to 5.7.3, and the router fix went in a day later without a second bump. So a 5.7.3 package built between those two commits would include the search fix and not the router fix. We downloaded the package JoomlaBoat serves now, dated September 2026, and it contains both. If you installed a 5.7.3 in late July, reinstall from the current download to be sure.

A gap like that between fix and CVE is normal: vendors fix first and the paperwork follows. It does mean that “there was no CVE yet” was never the same as “no one knew”. When a vendor’s changelog or commit history says “security”, treat the update as a security update on the day it ships.

Here is where the sites we monitor stand on the day the CVE was published: **not one connected Joomla site runs YouTube Gallery 5.7.3 yet.** Every install we can read a version from is on an affected build.

Is my Joomla site affected by CVE-2026-94130?

If a Joomla site has YouTube Gallery installed at any version below 5.7.3, yes. That includes the 5.x releases up to 5.7.2, the old 4.x free builds, and anything older. The installed component shows up in Joomla as “YouTube Gallery” or “Youtube Gallery”, with the element `com_youtubegallery`, and its author may read JoomlaBoat.com, Ivan Komlev or Design Compass corp depending on its age. They are all the same extension.

The extension ships with a content plugin, a module and an editor button, but the vulnerable queries live in the component. Updating the package to 5.7.3 fixes it. The same gallery pattern, an unauthenticated injection through a public search, is behind the OS Gallery flaws we disclosed earlier in September.

> **Most affected installs are on the old 4.x line**
>
> Across the Joomla sites we monitor, about three in four affected YouTube Gallery installs are on a version older than 5.0, and most of those sites run Joomla 3. There is no 4.x security release. The fix for those sites is the same 5.7.3 as everyone else, and in our data 5.x builds already run on Joomla 3.10 sites. JoomlaBoat lists PHP 7.4 as the minimum.

What you should do right now

1. **Update YouTube Gallery to 5.7.3** on every Joomla site that has it, from JoomlaBoat’s download page or through Joomla’s updater.
2. **Check the version afterwards.** In System, Manage, Extensions, the YouTube Gallery component should read 5.7.3.
3. **If you cannot update today,** disable the component, its content plugin and its module until you can. That removes the public search and the routed video URLs.
4. **Look for administrator accounts you did not create.** A SQL injection that can read the users table is a route to account takeover through password hashes and session data. Our walkthrough on finding rogue admin accounts in Joomla shows what to look for.
5. **If the gallery is no longer used, uninstall it.** An extension no one uses still answers requests from anyone who finds it.

Find administrator accounts you never created

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 →

How mySites.guru finds every YouTube Gallery install

The hard part of any extension vulnerability is knowing which of your sites run the thing, and at what version. mySites.guru keeps a live inventory of every extension on every connected Joomla site, so one search for YouTube Gallery returns every site with it installed and the version each one runs.

We added CVE-2026-94130 to our vulnerability database on the day it was published, so every connected site below 5.7.3 is flagged on its dashboard now, without anyone having to go looking. The mass updater then pushes the update to all of them from one screen. That is part of the subscription, and it works the same way across a portfolio of Joomla sites of any size.

Why old video galleries keep turning up in security advisories

Video and gallery extensions tend to be installed once, when the site is built, and then forgotten. They keep working, so no one opens the extension manager to look, and the version falls further behind every year. The version spread we see for YouTube Gallery shows it clearly: installs dating back to the 1.x and 2.x releases, and a big block of sites still running a 4.x build that has not changed in years.

It has happened to this component before. CVE-2014-4960, published in July 2014, was an unauthenticated SQL injection in the same component, through its `listid` and `themeid` parameters, affecting 4.x through 4.1.7. Twelve years on, we still see a handful of connected sites running builds older than that.

Those old installs are what an attacker scanning for a newly published CVE finds first. An unauthenticated front-end SQL injection needs nothing but the URL of a page that shows a gallery. If you manage client sites, this is the kind of extension worth auditing for, whether or not anyone remembers adding it.

If a site has already been hit, or you would rather someone else clean it up, fix.mySites.guru patches the site, audits it for backdoors and returns it to you for a single fixed fee. Our Joomla hacked guide covers what to check yourself.

Disclosure and credit

We did not find this flaw, and it is one of a long run of Joomla extension security issues this year. The CVE record credits Osman Hussein, Krzysztof Zając of CERT Polska, and Dick Snel of onvio.nl as finders, and was published by the Joomla CNA on 26 September 2026. We have seen no report of this flaw being exploited in the wild, and it is not on CISA's Known Exploited Vulnerabilities list as of the date of this post. The fix is YouTube Gallery 5.7.3.

Timeline

2026-07-26 — **Search query fix committed to JoomlaBoat's public repository**

The commit is titled "Security: Fixed SQL injection vulnerability in search functionality" and bumps the version to 5.7.3.

2026-07-27 — **Router fix committed**

"Security: Fixed SQL injection vulnerability in router." Both fixes are visible to anyone reading the repository.

2026-09-26 — **CVE-2026-94130 published by the Joomla CNA**

CVSS 4.0 9.3 Critical, versions 1.0.0 to 5.7.2 affected.

2026-09-26 — **mySites.guru flags every affected site**

The range is in our vulnerability database, so connected sites below 5.7.3 are flagged automatically.

Further Reading

- YouTube Gallery product page - JoomlaBoat's download page for 5.7.3.
- CVE-2026-94130 on cve.org - the CNA record with the affected range and vector.
- joomlaboat/YoutubeGallery on GitHub - the extension's public source, including both fix commits.
- CWE-89: SQL Injection - the underlying weakness class.
- OWASP SQL Injection Prevention Cheat Sheet - why quoting and parameterising beats stripping characters.

Frequently Asked Questions

What is CVE-2026-94130?

An unauthenticated SQL injection in the YouTube Gallery extension for Joomla by JoomlaBoat.com. The Joomla CNA published it on 26 September 2026 with a CVSS 4.0 score of 9.3 Critical. It affects every version from 1.0.0 to 5.7.2 and is fixed in 5.7.3.

Does an attacker need to log in?

No. The CVSS vector says no privileges and no user interaction are required. The vulnerable code sits in the component's public front end: the video search and the router that turns friendly video URLs back into database lookups.

I am on an old 4.x version of YouTube Gallery. Is there a 4.x patch?

No. JoomlaBoat maintains one line of development and the fix only exists in 5.7.3. Sites on 4.x or older have to move to 5.7.3. In our data, 5.x builds already run on Joomla 3.10 sites, so being on Joomla 3 is not by itself a reason to stay on 4.x. The vendor lists PHP 7.4 as the minimum.

What can an attacker get from this SQL injection?

Anything the Joomla database user can read. That normally includes every user account, email address and password hash, active session data, and the site's configuration stored in the database. The CNA scores confidentiality, integrity and availability impact all as High.

What should I do if I cannot update today?

Disable the YouTube Gallery component, its content plugin and its module until you can update, which removes the public entry points. Then update to 5.7.3 and check your administrator accounts for anything you did not create.

Who found it?

The CVE record credits three finders: Osman Hussein, Krzysztof Zając of CERT Polska, and Dick Snel of onvio.nl. We did not find this flaw; we cover it because many sites we monitor run the extension.

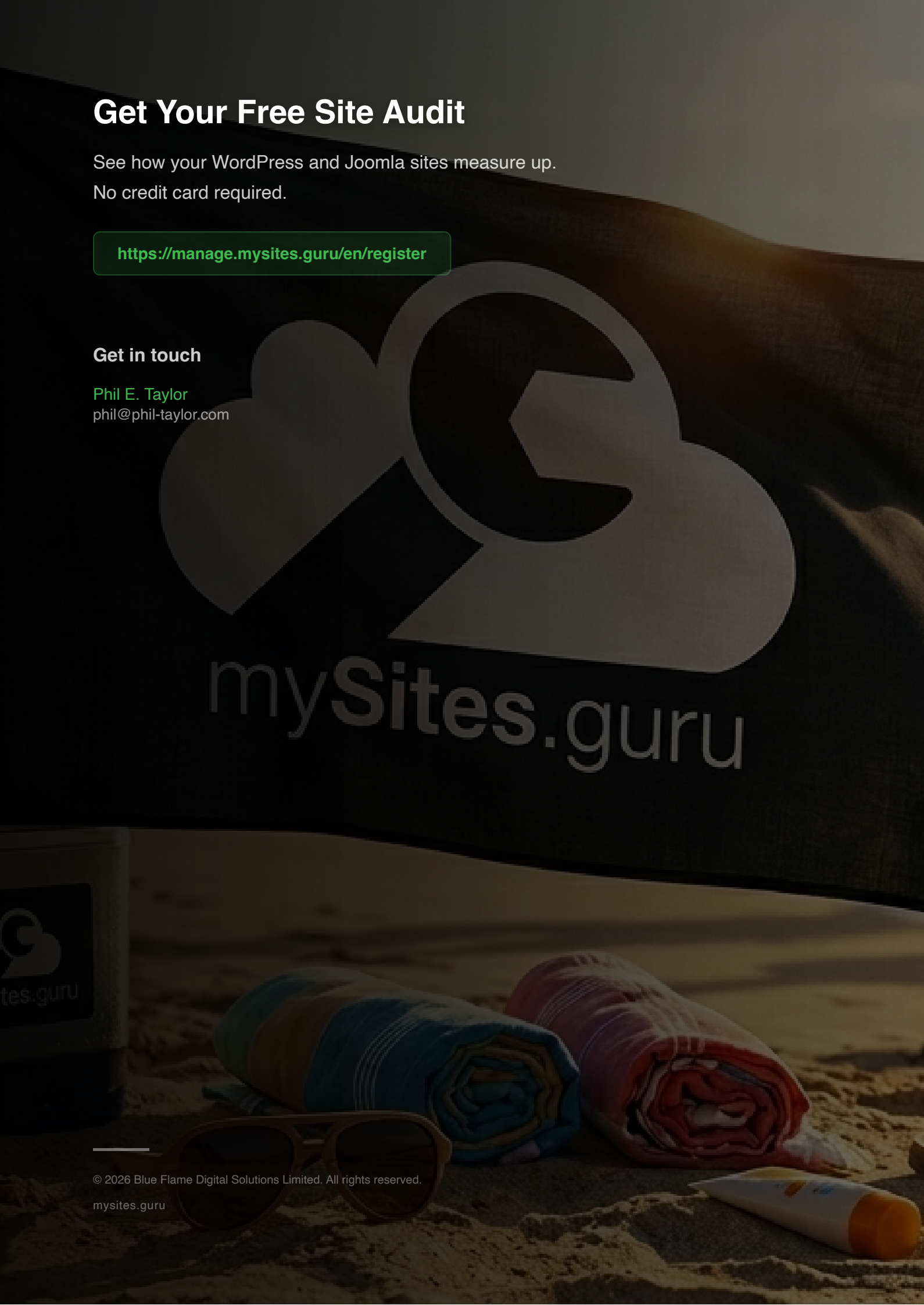
Written and edited by a human, with AI assistance. Our approach to AI

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