



JCTables for Joomla: Unauthenticated SQL Injection Fixed in 1.21.1

CVE-2026-76570 lets anyone read and rewrite a Joomla database through the JCTables extension without logging in. Scored 10.0 Critical, fixed in 1.21.1.

Phil E. Taylor | 30 September 2026

TL;DR

[CVE-2026-76570](#) is an unauthenticated SQL injection in [JCTables](#), JoomCode's datatables component for Joomla. The Joomla CNA published it on 30 September 2026 and scored it 10.0 Critical, the top of the scale. Every version before 1.21.1 is affected, and the fix is 1.21.1.

No login is needed, and the injection works in write queries as well as reads, so an anonymous visitor can change rows in the database as well as copy them. [VulnCheck's write-up](#) takes that as far as running code on the server. Update to 1.21.1.

10.0

CVSS 4.0

[CVE-2026-76570](#) Unauthenticated SQL injection in read and write queries

CRITICAL Joomla CNA

Any visitor can read any table in the Joomla database and change any row, which is enough to take over an administrator account.

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:A/AU:Y

No login needed

Read and write

All versions before 1.21.1

▼ 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: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

What went wrong in the JCTables front-end controller

JCTables lets a site show database tables to visitors and, if the site owner allows it, lets them edit cells inline. That editing runs through a front-end controller reached at `index.php?option=com_jctables&task=...`. Before 1.21.1, that controller checked neither who the visitor was nor Joomla's form token, on any of its tasks. The CVE record describes it as a "CRUD API controller" that "performs no Joomla token validation and no authentication check on any task."

The queries behind those tasks made it worse. According to [VulnCheck's analysis](#), the tasks that update cells, delete rows, insert and update records, save forms and fetch rows took table names, column names and values straight from the request. And the helper meant to escape those values, `ladb_escape()`, returned anything already wrapped in quote marks unchanged, on the theory that it must be escaped already.

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

The write half is what earns the 10.0. A read-only SQL injection gives an attacker a copy of your data. This one also lets them change it, including the administrator account's password hash. VulnCheck showed the full chain in a lab: rewrite an administrator's credentials, log in to the back end, install an extension, and run code as the web server.

A malicious actor's own code runs on your server, with the same access as the website itself: reading, changing or deleting any file it can touch, planting a backdoor that survives the next update, installing malware, pulling every database credential and API key from your configuration, and using your server to attack other people. Gulp.

That last step needs the Joomla administrator login page to be reachable, which it is on most sites. Changing the database needs no login at all.

What changed in JCTables 1.21.1

VulnCheck lists what JoomCode changed:

- Each write task now checks Joomla's form token with `Session::checkToken()`, so the component rejects a request that did not come from the site's own form.
- `ladb_escape()` now quotes the value through the database driver instead of trusting input that arrives already quoted. That is the pattern OWASP recommends: escape or bind each value instead of guessing which ones are already safe.
- Row reads are limited to tables the administrator has configured, instead of whatever table the request names.

JoomCode shipped the fix eight days after the report: VulnCheck reported it on 28 July 2026 and 1.21.1 was released on 5 August. That is a fast turnaround by any vendor's standard.

The JCTables fix was out for eight weeks before the CVE

The CVE arrived on 30 September, eight weeks after 1.21.1. For most site owners the CVE is the signal, because it is what scanners, alerts and news feeds pick up. So the

eight weeks in between were a window in which the fix existed and few site owners had a reason to install it.

Our data shows how that played out. **On the day the CVE was published, roughly seven in eight JCTables installs across the Joomla sites we monitor were still on an affected version.** Only about one in eight had moved to 1.21.1. Of the affected installs, more than two in three are on the older 1.10.x builds, not the 1.20.0 release just before the fix.

We see this pattern with most extension disclosures. The same thing happened with YouTube Gallery on 26 September 2026, where the fix sat in a public repository for two months before its CVE. When an extension update ships, the safest assumption is that it might be a security fix, whether or not anyone has said so yet.

Is my Joomla site affected by CVE-2026-76570?

If a Joomla site has JCTables installed at any version below 1.21.1, yes. That covers the 1.20.0 release, every 1.10.x build, and anything older. In Joomla it appears as "JCTables" or "JC Tables", with the element `com_jctables` and the author JoomCode.

The flaw is in the component. JoomCode also ships a "Content - JCTables" plugin that embeds tables in articles; the CVE does not name it, and the fix is in the component package. JoomCode's free download is [com_jctables 1.21.1 free.zip](#). Pro subscribers get their package from the same page after logging in.

Pro users: check the version number after updating

The CVE and VulnCheck's analysis describe the free edition, and the CNA's affected range does not split the editions. Rather than assume the Pro build is different, check that the JCTables component on each site reads 1.21.1 or later after you update.

What you should do right now

1. **Update JCTables to 1.21.1** on every Joomla site that has it, from [JoomCode's download page](#) or through Joomla's updater.
2. **Check the version afterwards.** In System, Manage, Extensions, the JCTables component should read 1.21.1.
3. **If you cannot update today,** disable the JCTables component until you can. That removes the vulnerable controller.
4. **Assume the database may have been read or changed** if an affected version was live. Change every administrator password, and our guide to [checking Joomla database security](#) covers what else to review.
5. **Look for administrator accounts you did not create, or existing ones that changed.** This flaw can write to the users table, so a new or altered super user is the first thing to rule out. Our walkthrough on [finding rogue admin accounts in Joomla](#) shows what to look for.
6. **If the component 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 JCTables install

The hard part of any extension vulnerability is knowing which of your sites run it, and at what version. mySites.guru keeps a live inventory of the extensions on each connected

Joomla site, so one search for JCTables lists the sites that have it installed and the version each one runs.

We added [CVE-2026-76570](#) to our [vulnerability database](#) on the day it was published, so every connected site below 1.21.1 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 Joomla data-table extensions are a high-value target

A datatables component exists to put database rows on a web page, and JCTables goes further than most: its own listing promises master-detail tables, inline editing and connections to external databases. That is a component whose job is building queries from what the page asks for. When that path is open to anonymous visitors, the distance from “a page with a table on it” to “the whole database” is very short.

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’s own JavaScript will ever call it. An attacker does not use the extension’s JavaScript. They call the endpoint directly. Listing and table components keep turning up for this reason: the [three OrdaSoft extensions with SQL injections in their sort order](#), published on 28 September 2026, built part of their queries from the request in much the same way.

If a site has already been hit, or you would rather someone else cleaned 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](#), several of them from [researchers auditing the same extensions we are](#). The

CVE record credits Valentin Lobstein (Chocapikk) as the finder, and VulnCheck published the technical write-up the same day the Joomla CNA published the record, 30 September 2026. VulnCheck reports no evidence of exploitation in the wild, and the flaw is not on CISA's Known Exploited Vulnerabilities list as of the date of this post. The fix is JCTables 1.21.1.

Further Reading

- VulnCheck: JCTables unauthenticated SQL read/write to RCE - the finder's technical write-up, including what the fix changed.
- CVE-2026-76570 on cve.org - the CNA record with the affected range and vector.
- JC Tables downloads at JoomCode - where the free 1.21.1 package lives.
- CWE-89: SQL Injection - the underlying weakness class.
- OWASP SQL Injection Prevention Cheat Sheet - why binding and quoting every value beats trusting input that already looks quoted.

Frequently Asked Questions

What is CVE-2026-76570?

An unauthenticated SQL injection in JCTables, the datatables component for Joomla by JoomCode. The Joomla CNA published it on 30 September 2026 with a CVSS 4.0 score of 10.0 Critical. Every version before 1.21.1 is affected, and 1.21.1 is the fix.

Does an attacker need to log in?

No. The CVSS vector says no privileges and no user interaction are required. The vulnerable tasks sit in the component's front-end controller, which did not check the visitor's login or Joomla's form token before running a query.

Is this only a data leak, or can an attacker change the site?

Both. The flaw is in read queries and in write queries. An attacker can read any table the Joomla database user can see, including the users table, and can change rows. VulnCheck, whose researcher found the flaw, showed that this is enough to take over an administrator account and from there install code on the server.

Which version of JCTables should I be on?

1.21.1 or later. JoomCode's free download is com_jctables_1.21.1_free.zip, released on 5 August 2026 according to VulnCheck. There is no separate patch for the older 1.10.x builds: 1.21.1 is the fix for them too.

What should I do if I cannot update today?

Disable the JCTables component until you can update, which removes the public entry point. Then update to 1.21.1, change your administrator passwords, and check your administrator accounts for anything you did not create.

Who found it?

The CVE record credits Valentin Lobstein (Chocapikk) of VulnCheck, who reported it to JoomCode on 28 July 2026. We did not find this flaw; we cover it because sites we monitor run the extension.

AI MODIFIED

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

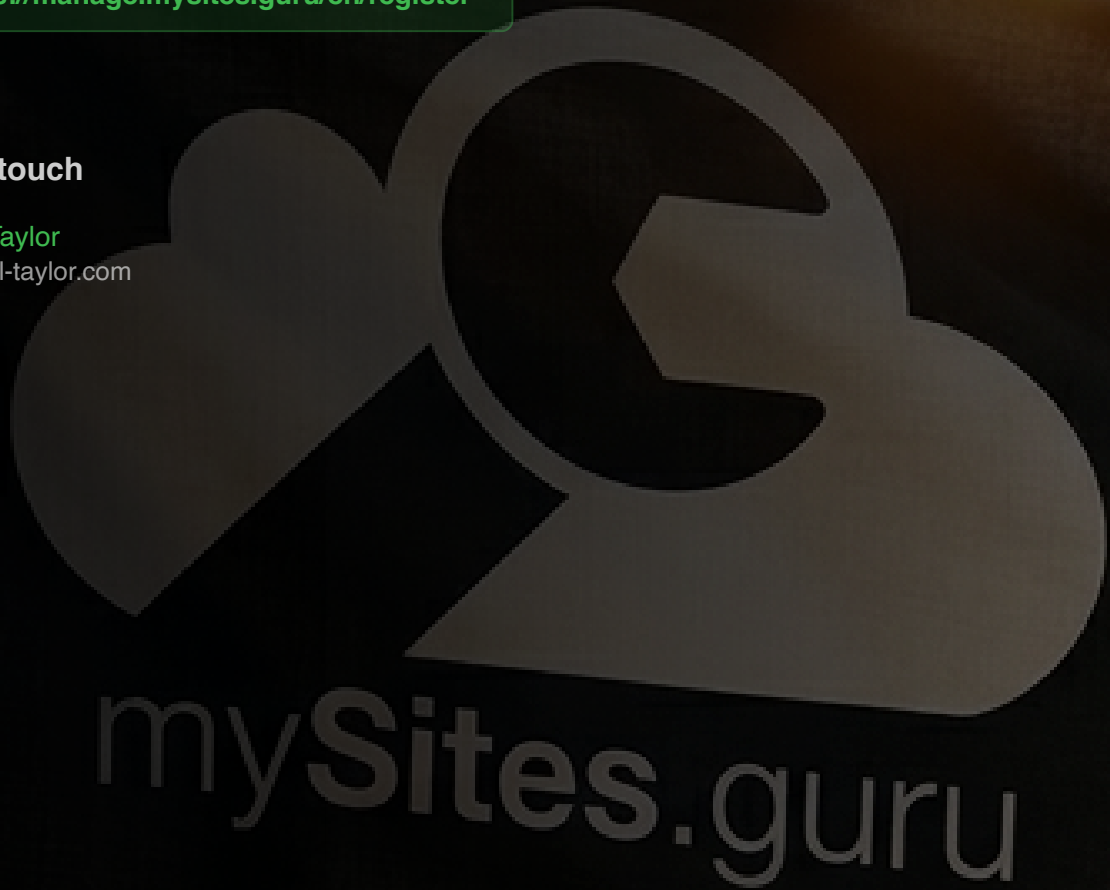
Get Your Free Site Audit

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

