



Gridbox 2.20.4.2 Fixes Two Unauthenticated SQL Injection Flaws

Gridbox 2.20.4.2 fixes two SQL injection flaws that need no login. About 95% of the Gridbox sites we monitor were affected. Update every Joomla site today.

Phil E. Taylor | 27 October 2026

TL;DR

Balbooa released Gridbox 2.20.4.2 on 27 October 2026 with two security fixes for the Joomla page builder, and both of them close a SQL injection flaw that an anonymous visitor can reach. One is in the sort order for store and category post lists. The other is in a page editor task that loads blog posts and had no permission check at all.

Balbooa says 2.20.4.1 and earlier are affected and rates the release Critical. The Joomla CNA published CVE-2026-102788 (the sort order injection) and CVE-2026-102789 (the missing editor permission check) the same morning, both scored CVSS 4.0 9.3 Critical. Neither needs a login, and about 95% of the Gridbox sites we monitor were on an affected version on the morning of the release. Update to 2.20.4.2 today.

9.3

CVSS 4.0

CVE-2026-102788 SQL injection through the store list sort order

CRITICAL Joomla CNA

An anonymous visitor can put their own SQL into the sort order of a store product list and read data out of the site database, including the Joomla user table.

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

CWE-89 SQL injection

1.0.0 to 2.20.4.1

▼ 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:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

9.3

CVSS 4.0

CVE-2026-102789 Missing permission check on an editor task

CRITICAL Joomla CNA

A page editor task that loads blog posts could be called by any visitor and passed its sort order into the same query, a second unauthenticated route to the SQL injection.

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

CWE-284 missing authorisation

1.0.0 to 2.20.4.1

▼ 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:N None: Other systems keep their data

SI:N None: Other systems keep their integrity

SA:N None: Other systems stay up

What do the two Gridbox fixes change?

The first fix, CVE-2026-102788, is to the sort order on store and category post lists. A visitor can ask for those lists sorted in different ways through the page URL, and in 2.20.4.1 the value they supplied went into the ORDER BY part of the database query

that lists the posts. In 2.20.4.2 the value is checked against a strict whitelist of allowed sort options, and anything that is not on the list falls back to a safe default. Balbooa describes this as preventing SQL injection, and that matches what we see in the code.

The second fix, [CVE-2026-102789](#), is to one of the page editor's tasks, the one that loads blog posts for the editor to show. In 2.20.4.1 that task had no login or permission check, so an anonymous visitor could call it, and it passed its own sort value into the same query. 2.20.4.2 adds a permission check so that guests are turned away before the query runs. Balbooa describes this as restricting unauthenticated guest access, which is accurate but undersells it: without the check, the editor task was a second front door to the same SQL injection.

We compared the public 2.20.4.2 package with 2.20.4.1. Only two PHP files changed, and each of them is one of the two fixes above. Both confirm Balbooa's description, and there is nothing else to configure after updating.

Why an ORDER BY injection still matters

An injection into the sort order of a query is sometimes waved away because it does not sit in the WHERE clause, where the classic textbook attacks go, but a database will happily evaluate an expression in ORDER BY, and an attacker who controls that expression can make the result order depend on a question about any other table. Ask enough yes-or-no questions and you have read the answer, one character at a time.

Both of these flaws are read-side: what an attacker gets is data read out of the database, and on a Joomla site that includes the user table with its password hashes, and every other table the extensions on the site have created.

Read-only is not the same as harmless

A SQL injection that only reads still hands over the user table. Password hashes can be worked on offline and email addresses can be used to phish your administrators. Nothing about the attack has to break the site, so you cannot count on an error to tip you off.

The sort order keeps turning up in Joomla extension flaws

Gridbox is the latest of several Joomla extensions this year with an unauthenticated SQL injection through the sort order of a public listing. In July it was [EasyStore](#), which put request input straight into a query's `ORDER BY`, and [SP Page Builder](#), whose Dynamic Content endpoint appended a sort direction from the request. [Fabrik 4.7.2](#) fixed one in its list ordering in August. In September came [SP Property Finder](#), then [three OrdaSoft extensions](#) (Book Library, Real Estate Manager and Vehicle Manager) on one day, then [OS CCK](#) two days later.

The same thing goes wrong each time. Joomla's quoting functions protect a value that sits inside quotes, such as a search term. A sort column or direction is part of the query's structure and sits there unquoted, so quoting does not help, and a developer who has been careful everywhere else can still leave this one open. The fix Balbooa chose here is the right one: compare the requested sort against a fixed list of allowed options and ignore anything else. If you build Joomla extensions, search your own code for sort values taken from the request.

Which Gridbox versions are affected?

Balbooa's note says 2.20.4.1 and earlier are affected, with the fix in 2.20.4.2. Our newest rule flags 2.20.4.0 and 2.20.4.1 with both CVE numbers, and the older Gridbox rules have been repointed so that every earlier build now names 2.20.4.2 as the version to install.

Gridbox version	Status	What to do
2.20.4.2	Fixed	Nothing
2.20.4.0 to 2.20.4.1	Affected by this release's two fixes	Update to 2.20.4.2
2.20.3.1 and below	Also exposed to the language install CSRF and image preview path check	Update to 2.20.4.2

Gridbox version	Status	What to do
Below 2.20.2	Exposed to the actively exploited July flaws	Update to 2.20.4.2 urgently and check for compromise

Sites on the Joomla 3 line top out at Gridbox 2.17.0.2, which has no fix for any of this year's flaws. For those sites the fix is moving to a supported Joomla.

What you should do right now

1. Update Gridbox to 2.20.4.2 on every Joomla site that runs it, through Joomla's Update tab or the mySites.guru mass updater.
2. Confirm the version afterwards: open System, Manage, Extensions and check that Gridbox reads 2.20.4.2.
3. If a site sat on an affected version and you are worried about it, look for administrator accounts you did not create. A SQL injection that reads the user table gives an attacker the material to work towards a login, and a new Super User is the usual end point.
4. Consider resetting the passwords of your administrator accounts on those sites. It costs a few minutes and removes the value of anything that was read.

There is no public report of exploitation yet, and this post does not say that any site has been compromised. The checks above are what you do when you cannot rule it out.

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.

How do I find every Gridbox site I manage?

mySites.guru keeps a live inventory of the extensions on each connected Joomla and WordPress site. Search for Gridbox once and you get every site running it, the version each is on and whether an update is waiting. On the morning of the release, about 95% of the Gridbox sites we monitor were on an affected version. About four in five were on 2.20.4.1, the release from 21 October, and fewer than 1% had already moved to 2.20.4.2.

Most Gridbox sites moved to 2.20.4.1 within six days of its release, so the update habit is there; it needs one more round. Connected sites on 2.20.4.0 and 2.20.4.1 are flagged automatically with both CVE numbers, and the [mass updater](#) pushes 2.20.4.2 to all of them from one screen. That is part of the [subscription](#), not a separate purchase.

Five Gridbox security releases since July

2.20.1 fixed the [cookie authentication bypass](#) in July. 2.20.2 fixed the [23 flaws from our audit](#) later that month. 2.20.3.1 fixed the [blog author SQL injection](#) on 21 September. 2.20.4.0 fixed the [language install CSRF and image preview path check](#) on 8 October. 2.20.4.2 is the fifth.

Look at the two SQL injection fixes side by side and a pattern appears. 2.20.3.1 closed an injection through the author parameter in the public blog post listing code. 2.20.4.2 closes one through the sort order in the same listing code, five weeks later. Both come down to the same mistake in the same public post listings: a value from the request reaching the query without being checked against a list of what is allowed. When a fix addresses the one parameter that was reported rather than the pattern, the next parameter over is the obvious place for the next researcher to look, and that is what

happened here. If your Gridbox sites went to 2.20.4.1 six days ago, they need updating again today.

Disclosure and severity

This is not a mySites.guru finding. Balbooa credits Artur Błażewicz for reporting the issues, and David Jardin of the Joomla Security Strike Team for coordinating the disclosure.

Balbooa rates the release Critical, and the Joomla CNA agrees: [CVE-2026-102788](#) (CWE-89, SQL injection) and [CVE-2026-102789](#) (CWE-284, missing authorisation) are both scored CVSS 4.0 9.3 Critical, with every release from 1.0.0 to 2.20.4.1 listed as affected. Our own reading would score them a little lower, at 8.7 High, because what we can see in the code is a read-side injection, and the CNA's vector also rates integrity and availability High. We quote the record's score, because that is what scanners and other advisories will show you. Either way, both flaws need no login and should be patched today.

If a site has already been hit, or you would rather someone else made sure, [fix.mySites.guru](#) patches the site, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Timeline

-
- 2026-09-21** ○ **Gridbox 2.20.3.1 fixes an unauthenticated blog author SQL injection**
The first SQL injection fix in the public blog post listing code.
 - 2026-10-08** ○ **Gridbox 2.20.4.0 fixes a language install CSRF and an image preview path check**

		Reported by Sergiy Tryzhychynskyi, coordinated by the Joomla Security Strike Team.
2026-10-21	○	Gridbox 2.20.4.1 released About four in five of the Gridbox sites we monitor were on this version by the morning of 27 October.
2026-10-27	○	Gridbox 2.20.4.2 fixes two unauthenticated SQL injection flaws Reported by Artur Błażewicz, coordinated by David Jardin of the Joomla Security Strike Team. The Joomla CNA publishes CVE-2026-102788 and CVE-2026-102789 the same morning, both CVSS 4.0 9.3 Critical.
2026-10-27	●	mySites.guru flags every affected site Connected sites on 2.20.4.0 and 2.20.4.1 are flagged automatically with both CVE numbers, and the older Gridbox rules now point to 2.20.4.2.

Further Reading

- [Balbooa: Gridbox 2.20.4.2. Security Hardening Update](#) - the vendor's own release note.
- [Gridbox 2.20.4.0 Fixes a Language Install CSRF and an Image Path Check](#) - the previous release, 19 days earlier.
- [Blind SQL Injection in Gridbox's Blog Author](#) - the 2.20.3.1 fix in the same listing code.
- [Another 23 Critical Security Vulnerabilities in Gridbox for Joomla](#) - the July audit.
- [Gridbox for Joomla: One Cookie and You Are a Super User](#) - the July authentication bypass.
- [OWASP: SQL Injection](#) - how SQL injection works and why whitelists stop it.

- CWE-89: Improper Neutralization of Special Elements used in an SQL Command
 - the underlying weakness class.

Frequently Asked Questions

What does Gridbox 2.20.4.2 fix?

Two SQL injection flaws in the Joomla extension, both reachable without an account. The sort order for store and category post lists is now checked against a strict whitelist, and a page editor task that loads blog posts now has a permission check. Balbooa credits Artur Błażewicz for reporting them, with David Jardin of the Joomla Security Strike Team coordinating.

Which Gridbox versions are affected?

Balbooa lists 2.20.4.1 and earlier as affected, and the fix is 2.20.4.2. Our own comparison of the 2.20.4.2 and 2.20.4.1 packages confirms the two changed areas. Sites below 2.20.2 also have the actively exploited July flaws and should go straight to 2.20.4.2.

Can an anonymous visitor exploit these flaws?

Yes. The sort order is read from the public page URL, and the editor task that was changed had no login or permission check at all. Both flaws let an attacker read data from the database without an account, which is why we say patch today rather than at the next maintenance window.

Is there a CVE?

Yes, two, published by the Joomla CNA on the morning of the release. [CVE-2026-102788](#) is the SQL injection through the store list sort order and [CVE-2026-102789](#) is the missing permission check on the editor task. Both are scored CVSS 4.0 9.3 Critical and list every release from 1.0.0 to 2.20.4.1 as affected.

Have these flaws been exploited?

There is no public report of exploitation yet. Neither Balbooa nor the Joomla Security Strike Team has said anything either way, and neither CVE is on the CISA KEV list. A read-only SQL injection leaves little trace in the site itself, so if a site sat on an affected version, check for administrator accounts you did not create and consider resetting admin passwords.

AI MODIFIED

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

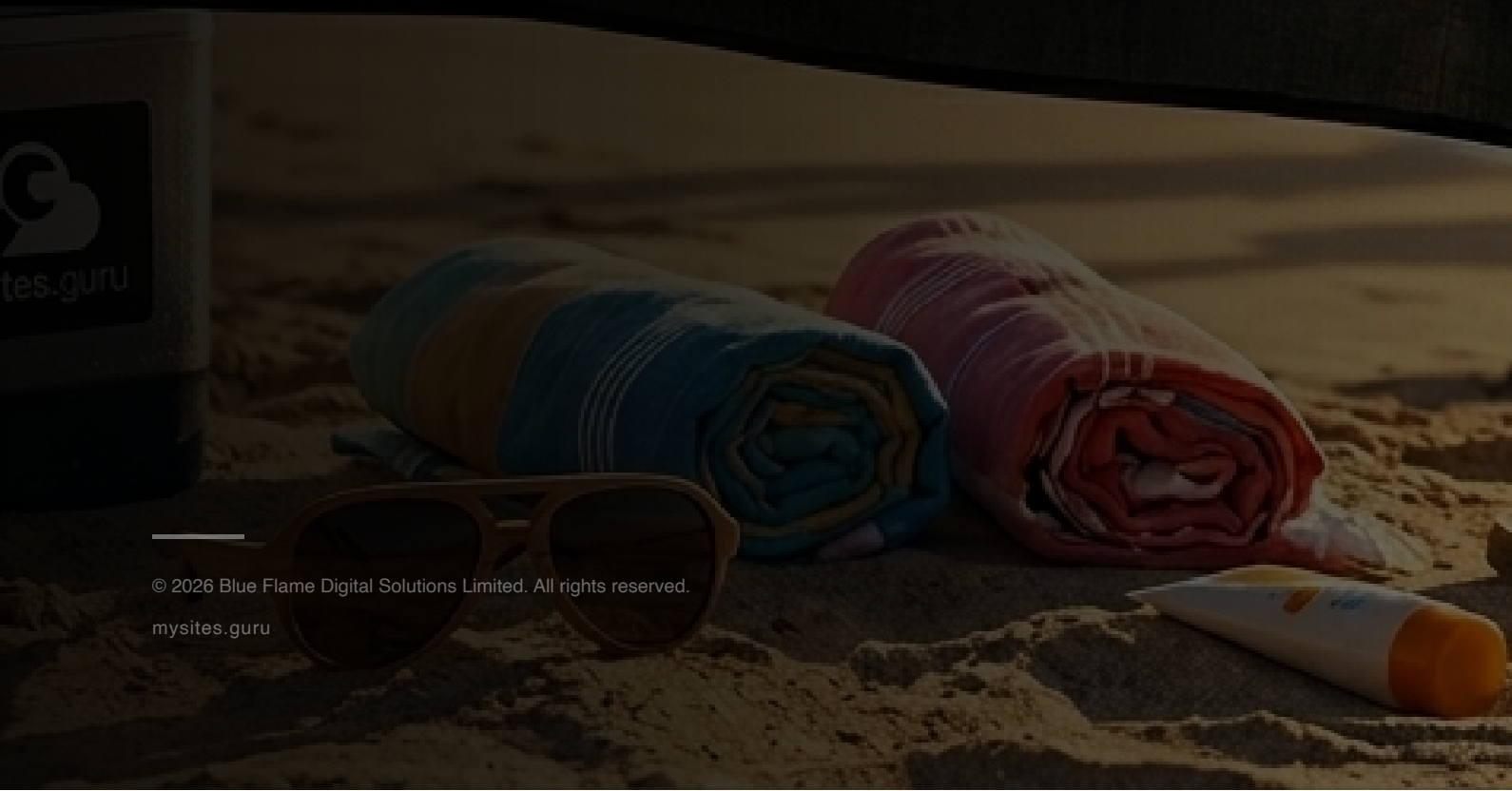
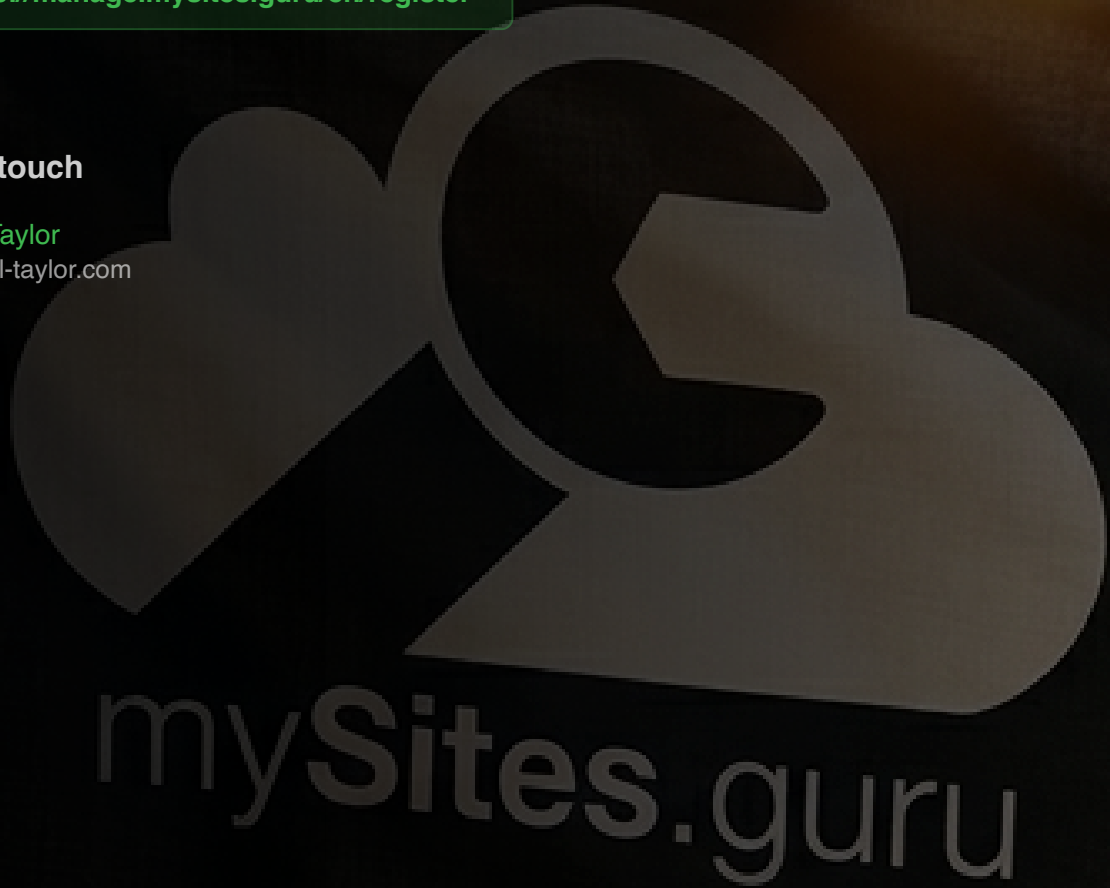
Get Your Free Site Audit

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