



Gridbox 2.20.4.0 Fixes a Language Install CSRF and an Image Path Check

Gridbox 2.20.4.0 fixes a CSRF flaw in language installation and tightens image preview path checks. Every Joomla site on 2.20.3.1 or older should update.

Phil E. Taylor | 8 October 2026

TL;DR

Balbooa released Gridbox 2.20.4.0 on 8 October 2026 with two security fixes for the Joomla page builder. The bigger one is a Cross-Site Request Forgery (CSRF) flaw in the language installation process. The smaller one tightens the path check in the image preview so it only serves images from the configured media folder.

The version most Gridbox sites run today, 2.20.3.1, is affected, and so is every 2.20.2.x and 2.20.3 build before it. Update to 2.20.4.0. There is no CVE and no CVSS score yet. Our own severity call is High, because the CSRF flaw ends with software installed on the site, even though it needs a Super User to be tricked into it.

The language installation CSRF

Gridbox lets an administrator install extra interface languages from inside the component. Installing a language means installing a Joomla package, which is the same machinery that installs any extension, so the action is limited to Super Users.

Cross-Site Request Forgery is an attack on the person rather than the server. The attacker cannot log in, so instead they get someone who already is to send a request on their behalf, usually by getting them to open a link or visit a page while their admin session is live. Joomla's defence is a per-session token that every state-changing request must include. A request forged from another site does not have the token, so Joomla rejects it.

Gridbox 2.20.2 added that token check across its admin controllers as part of fixing the 23 vulnerabilities from our July audit. The language installation action had a route around that check. 2.20.4.0 closes that path, so the token check now covers the language install as well.

Why an admin-only flaw still rates High

A Super User has to be signed in and has to open the attacker's link, so this cannot be sprayed at a site the way an unauthenticated flaw can. But the action installs software. If it works, the attacker's code runs on the site with the same access as any extension you installed yourself. Admins open links all day, in support tickets, contact form messages and emails, and one of them is all it takes.

The image preview path check

The second fix is narrower. Gridbox's image preview serves an image from the site so the editor can show it, and it is meant to stay inside the media folder configured in Gridbox. The containment check in 2.20.2 to 2.20.3.1 was looser than intended, and in some folder layouts it accepted image paths outside that folder. 2.20.4.0 makes the comparison exact.

The preview only serves image files, so `configuration.php` and other PHP files were not reachable through it. It tightens the containment added in July.

Which Gridbox versions are affected?

We compared the public 2.20.4.0 package with 2.20.3 and 2.20.2.2. Both of the changed areas are present from 2.20.2 onwards, so our rule flags 2.20.3.1, and the existing rules for earlier ranges now point to 2.20.4.0 as the version to install.

Gridbox version	Status	What to do
2.20.4.0	Fixed	Nothing
2.20.3.1	Affected by this release's two fixes	Update to 2.20.4.0
2.20.2.3 to 2.20.3	Also exposed to the blog author SQL injection	Update to 2.20.4.0
Below 2.20.2	Exposed to the actively exploited July flaws	Update to 2.20.4.0 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 2.20.4.0** 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 Gridbox reads 2.20.4.0.
3. **Check for extensions you did not install.** If you are worried a Super User on one of your sites opened something they should not have, look at the extensions list for anything unexpected, and at administrator accounts you did not create.
4. **If you use Facebook login,** generate a new App ID and App Secret. Balbooa reworked the integration for Facebook's API changes, so the old ones will not work.
5. **Check your image compression settings.** They have moved from Media Manager settings to Performance Tools, Images, and now apply to image uploads anywhere in Gridbox.

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 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 the sites running it, the version each is on and whether an update is waiting. Across the Joomla sites we monitor, several hundred run Gridbox, and the large majority were on 2.20.3.1 on the morning of the release.

We have added 2.20.3.1 to our vulnerability database, so connected sites still on it are flagged automatically, and the [mass updater](#) pushes 2.20.4.0 to all of them from one screen. That is part of the [subscription](#), not a separate purchase.

Four 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 at the end of that month. 2.20.3.1 fixed the blog author SQL injection three weeks ago. 2.20.4.0 is the fourth, and both of its fixes are follow-ups to protections that 2.20.2 introduced: the CSRF token check and the image path containment.

That pattern is normal once a large codebase gets serious attention. The first round of fixes adds the right protections, and outside researchers then find the corners those protections missed. The sites that get hurt are the ones that stopped updating after the first round. If your Gridbox sites went to 2.20.3.1 three weeks ago, they need updating again today.

Disclosure and severity

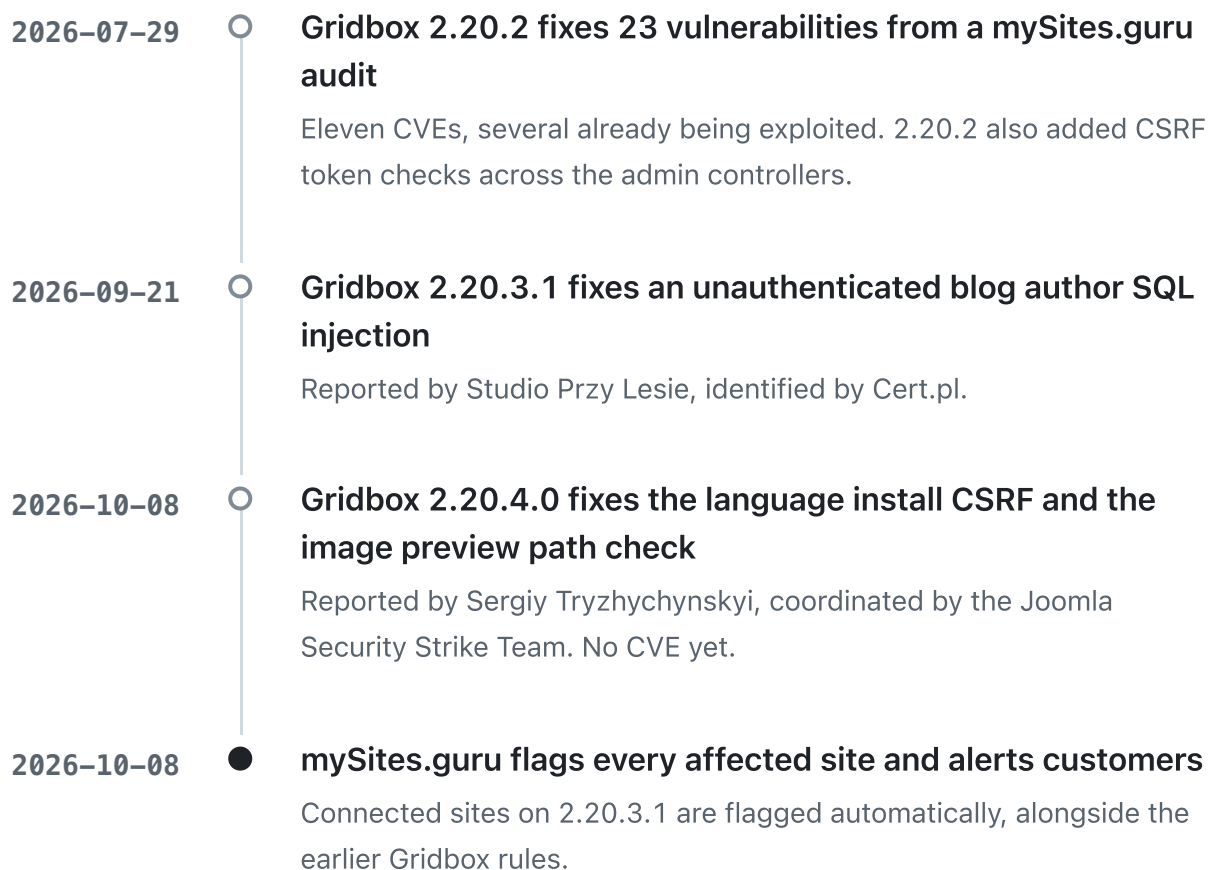
This is not a mySites.guru finding. Balbooa credits Sergiy Tryzhychynskyi for reporting both issues, and David Jardin of the Joomla Security Strike Team for coordinating the disclosure. Sergiy also reported part of the [Balbooa Forms 2.4.3.4 fixes](#) last month.

There is no CVE and no published CVSS score as of 8 October 2026, and Balbooa's note gives no affected range. Our assessment is High, driven by the CSRF flaw: it needs a signed-in Super User to cooperate unknowingly, which keeps it below Critical, but success means attacker-chosen software installed on the site. The image preview fix

on its own would be Low. We set the affected range from the code rather than waiting for a record, so connected sites are flagged 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

- 
- A vertical timeline with a central line and circular markers. The markers are open circles for updates and a solid black circle for the final action. Each entry includes a date on the left, a title in bold, and a description on the right.
- 2026-07-29** ○ **Gridbox 2.20.2 fixes 23 vulnerabilities from a mySites.guru audit**
Eleven CVEs, several already being exploited. 2.20.2 also added CSRF token checks across the admin controllers.
 - 2026-09-21** ○ **Gridbox 2.20.3.1 fixes an unauthenticated blog author SQL injection**
Reported by Studio Przy Lesie, identified by Cert.pl.
 - 2026-10-08** ○ **Gridbox 2.20.4.0 fixes the language install CSRF and the image preview path check**
Reported by Sergiy Tryzhychynskyi, coordinated by the Joomla Security Strike Team. No CVE yet.
 - 2026-10-08** ● **mySites.guru flags every affected site and alerts customers**
Connected sites on 2.20.3.1 are flagged automatically, alongside the earlier Gridbox rules.
-

Further Reading

- [Balbooa: Gridbox 2.20.4.0 New Features and Security Hardening](#) - the vendor's own release note.
- [Blind SQL Injection in Gridbox's Blog Author](#) - the 2.20.3.1 fix three weeks earlier.
- [Another 23 Critical Security Vulnerabilities in Gridbox for Joomla](#) - the July audit and its eleven CVEs.
- [Gridbox for Joomla: One Cookie and You Are a Super User](#) - the July authentication bypass, [CVE-2026-61425](#).
- [OWASP: Cross Site Request Forgery](#) - how CSRF works and why token checks stop it.
- [CWE-352: Cross-Site Request Forgery](#) - the underlying weakness class.

Frequently Asked Questions

What does Gridbox 2.20.4.0 fix?

Two security issues. A Cross-Site Request Forgery (CSRF) flaw in the language installation process, and weak file path validation in the image preview, which could serve images from outside the configured media folder. Balbooa credits Sergiy Tryzhychynskyi for reporting both, with the Joomla Security Strike Team coordinating.

Which Gridbox versions are affected?

Our reading of the code puts both flaws in every release from 2.20.2 up to and including 2.20.3.1, which is the version most Gridbox sites run today. The fix is 2.20.4.0. Sites below 2.20.2 have far more serious, actively exploited flaws and should go straight to 2.20.4.0 as well.

Can an anonymous visitor exploit the CSRF flaw?

Not on their own. CSRF works by getting someone who is already logged in to send a request they did not mean to send, and the language installation action is limited to Super Users. An attacker needs a Super User to open a crafted link or page while signed in to the Joomla administrator. The action installs software, so a successful attack puts code the attacker chose on the site.

Is there a CVE?

Not as of 8 October 2026. Balbooa published no CVE, no CVSS score and no affected-version range. The Joomla Security Strike Team coordinated the disclosure, so a CVE from the Joomla CNA may follow, and we will map it to our rule when it does.

Do I need to reconfigure anything after updating?

Only if you use Facebook login. 2.20.4.0 brings Google and Facebook social login back, but Facebook's API changes mean you need a new App ID and App Secret. Image compression has also moved from Media Manager settings to Performance Tools, so check your settings there.

AI MODIFIED

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

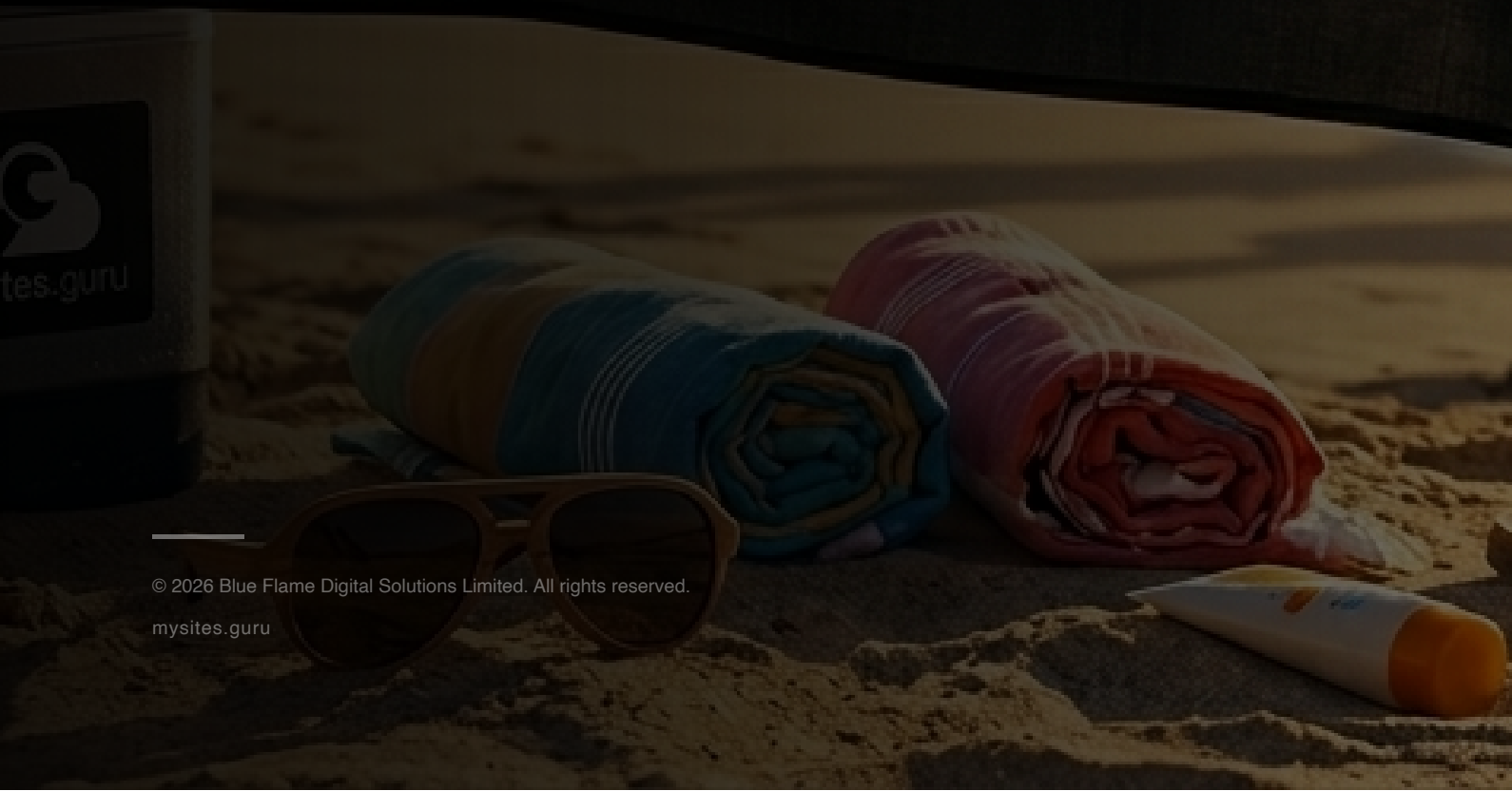
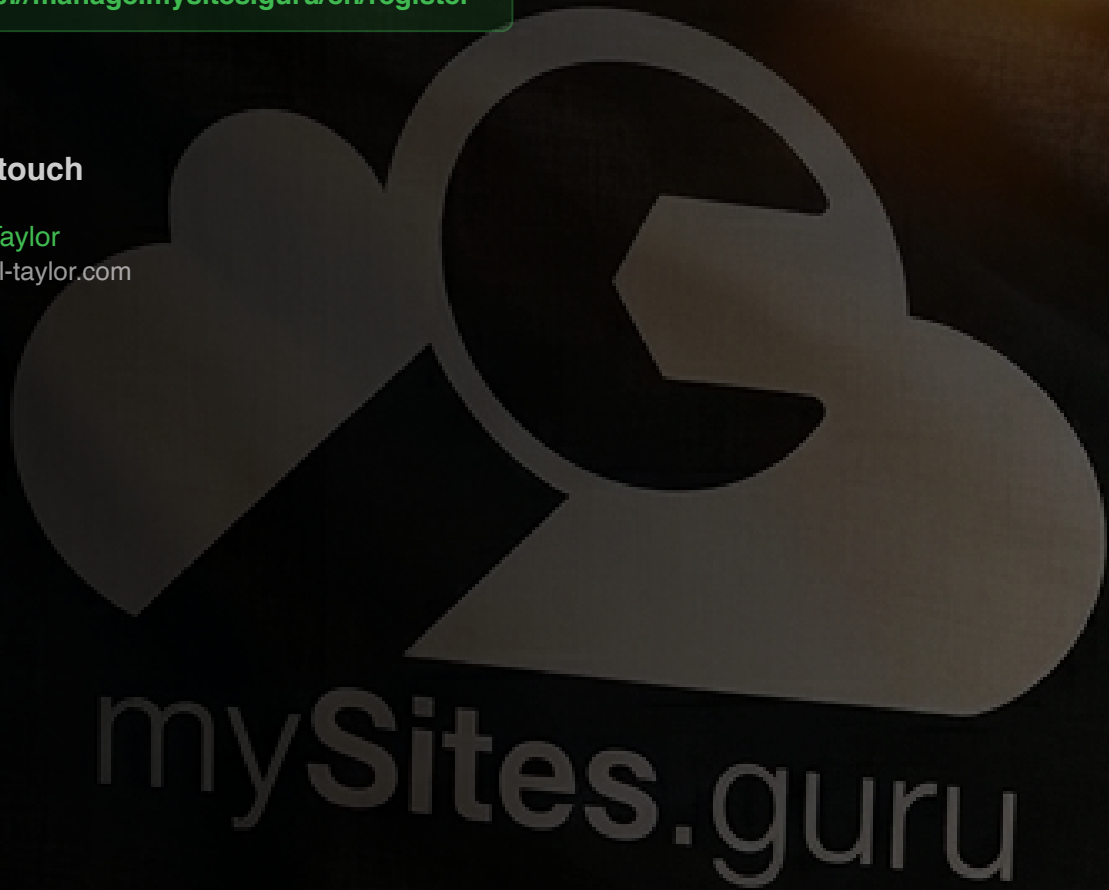
Get Your Free Site Audit

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