Blind SQL Injection in Gridbox's Blog Author

Gridbox 2.20.3.1 fixes an unauthenticated blind SQL injection in the blog author parameter that can read a Joomla site's whole database. Update now.

Phil E. Taylor | 21 September 2026

TL;DR

Balbooa shipped Gridbox 2.20.3.1 on 21 September 2026. It fixes a time-based blind SQL injection in the blog `author` parameter, which lives on the public front end of any Gridbox blog and needs no login. An attacker can read your database one answer at a time, which is slow but reaches everything in it.

Every version below 2.20.3.1 is affected, which is nearly every Gridbox site in the mySites.guru database. There is no CVE and no CVSS score yet, and the vendor filed it as “security hardening”. Update to 2.20.3.1 now. If you are still below 2.20.2, you have a bigger problem than this one, covered in our two earlier Gridbox posts.

What the flaw is

Gridbox blogs let a visitor filter posts by author, with a URL like `index.php?option=com_gridbox&view=blog&author=5`. That `author` value went straight into a database query without being turned into a number or quoted first. When user input reaches a query as raw text, an attacker can stop describing an author and start writing SQL, and the database runs it.

The fix, visible by comparing the 2.20.3.1 release against 2.20.3, is a single change in the component’s router. The parameter is now cast to an integer before it reaches the query:

```
// Before (vulnerable): the author value is concatenated in as-is
->where('`id` = '.$query['author']);

// After (2.20.3.1): cast to an integer first, so only a number survives
->where('`id` = ' . (int) $query['author']);
```

The same casting was added to the neighbouring `tag`, `app` and `id` parameters in the router. Casting to an integer is the correct, complete fix for a numeric identifier: after it,

`author=5 AND SLEEP(10)` becomes the number `5` and nothing else.

Why a blind injection still reads everything

This is a blind injection, so it does not print database rows back on the page. It is time-based, which is the patient variant. The attacker phrases each question so a true answer makes the database pause and a false answer does not, then reads the answer from the response time. “Is the first character of the admin password hash an `a`?” Wait and see. Then the second character, and the next account, and the next table.

It is slower than an injection that dumps rows in one response, but it is not weaker. Given time, a time-based blind injection reads usernames, email addresses, password hashes, session tokens and site configuration, and it does all of it without a single valid login.

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

Is my Gridbox site affected?

If any Joomla site you run has Gridbox below 2.20.3.1, yes. The current 2.20.3 build and the 2.20.2.3 build before it are both affected, and so is every older release. The fix is 2.20.3.1 and nothing lower.

Below 2.20.2 is a different, worse conversation

Sites still running a Gridbox below 2.20.2 are exposed to the July 2026 set of flaws, several of which were being exploited in the wild, including a pre-auth remote code execution and an authentication bypass that handed out Super User access. Updating to

2.20.3.1 fixes all of it at once, but treat those sites as urgent and read the 23-vulnerability write-up and the authentication bypass post for what to check.

What you should do right now

1. **Update Gridbox to 2.20.3.1** 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 on the site and check Gridbox reads 2.20.3.1, so a half-applied update does not leave you exposed.
3. **Check your administrator accounts and users.** A flaw that can read password hashes and session tokens is a route to account takeover, so look for accounts you did not create and sessions you do not recognise.
4. **If you cannot update immediately,** unpublish any front-end Gridbox blog view that exposes the author filter until you can, which removes the reachable path.

How do I find every Gridbox site I manage?

The awkward question after any extension flaw is which of your sites actually run the thing. Past a handful of sites, logging into each Joomla admin to read the extensions list

is not realistic, and that is exactly how old versions survive.

mySites.guru keeps a live inventory of every extension, template and framework on every connected Joomla and WordPress site. Search for Gridbox once and get back every site running it, the version each is on and whether an update is waiting. Across the Joomla sites we manage, several hundred run Gridbox, which is a lot of sites to reach one at a time.

We have added the affected range, every version below 2.20.3.1, to our vulnerability database, so every connected site still on a vulnerable Gridbox is flagged automatically, and the mass updater pushes 2.20.3.1 to all of them from one screen. Finding and fixing the whole set is part of the subscription, not a separate purchase.

The third Gridbox security story in two months

This is the third security release for Gridbox since July. The authentication bypass came first, fixed in 2.20.1. Then Balbooa asked us to audit the extension and we reported twenty-three vulnerabilities, fixed in 2.20.2, several of which were already being exploited. Now an outside researcher, Studio Przy Lesie, has brought this SQL injection to Balbooa, with Cert.pl identifying it, fixed in 2.20.3.1.

Read that sequence the right way. An extension getting fixes is a sign of attention, not neglect, and the same Media Manager code has been hardened across Balbooa's Forms and Gallery products in the same window. The lesson for a site owner is not "drop Gridbox", it is that a popular page builder is a large attack surface, and staying current on it is not optional. The sites that get hurt are always the ones a version or two behind when the next one arrives.

No CVE, no CVSS, no advisory with a range

We did not find this flaw, so this is not our timeline to narrate. What we can say is what the disclosure does and does not tell a site owner. Balbooa's note names the vulnerability type and thanks the reporters, which is more than the July authentication

bypass changelog managed. It still ships with no CVE, no CVSS score and no statement of which versions are affected or whether the flaw is reachable without a login. A site owner reading it cannot tell how urgent it is or which of their sites are in scope.

That gap is why our own severity call and our own version range matter here. We read the code, confirmed the parameter and the fix, and set the affected range ourselves so the sites we manage are flagged correctly today rather than whenever a CVE catches up. Cert.pl is a CNA, so a record may follow; if it does, we will map it.

Stay ahead of the next one

Extension flaws are not rare events you can respond to one at a time. There has been one for Gridbox roughly every three weeks since July, and that is one extension among the dozens on a typical Joomla site. mySites.guru watches the whole set, flags a site the moment a version it runs becomes known-vulnerable, and lets you update everything from one place.

If a site has already been hit, or you would rather someone else make 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. Non-subscribers get a free month with it.

Disclosure and severity

There is no CVE and no published CVSS score for this flaw as of 21 September 2026. Our own assessment is High: the injection is unauthenticated, reachable on the public front end of any Gridbox blog, and can read the entire database, which is limited only by an attacker’s patience rather than by any access control. We are treating it with the same urgency as an equivalent scored flaw because “no number yet” is not the same as “not serious”.

Credit for the finding goes to Studio Przy Lesie for reporting it and Cert.pl for identifying it, per Balbooa’s release note. The fix is Gridbox 2.20.3.1.

Timeline

2026-07-20 — **Gridbox 2.20.1 fixes an unauthenticated authentication bypass**

CVE-2026-61425. One cookie made any visitor a Super User.

2026-07-29 — **Gridbox 2.20.2 fixes 23 vulnerabilities from a mySites.guru audit**

Eleven CVEs, several already being exploited.

2026-09-21 — **Gridbox 2.20.3.1 fixes the blog author SQL injection**

Reported by Studio Przy Lesie, identified by Cert.pl. No CVE, no CVSS, no advisory range published.

2026-09-21 — **mySites.guru flags every affected site and alerts customers**

The affected range is in our vulnerability database, so connected sites below 2.20.3.1 are flagged automatically.

Further Reading

- Balbooa: Gridbox 2.20.3.1 Bug Fixes and Security Hardening - the vendor's own release note.
- Gridbox for Joomla: One Cookie and You Are a Super User - the July authentication bypass, CVE-2026-61425.
- Another 23 Critical Security Vulnerabilities in Gridbox for Joomla - the audit that found eleven CVEs' worth of flaws.
- A month of Joomla extension vulnerabilities - the wider run of findings this is part of.

- Front-end AJAX endpoints are a CMS security blind spot - why an anonymous request can reach a database query.
- CWE-89: SQL Injection - the underlying weakness class.
- ISO/IEC 29147: Vulnerability disclosure and the CERT Guide to Coordinated Vulnerability Disclosure - what a full advisory should have contained.

Frequently Asked Questions

What does Gridbox 2.20.3.1 fix?

A time-based blind SQL injection in the front-end blog author parameter. Because it sits on the public front end of any Gridbox blog, it needs no login, no account and no token. Balbooa credits Studio Przy Lesie for reporting it and Cert.pl for identifying it.

Which Gridbox versions are affected?

Everything below 2.20.3.1. In practice that is almost every Gridbox site in the mySites.guru database: the current 2.20.3 and 2.20.2.3 builds are both affected, and so is anything older. The fix is 2.20.3.1. Note that sites still below 2.20.2 have a far more serious problem, the July 2026 set of actively exploited flaws, and should read our other two Gridbox posts.

Is there a CVE for this?

Not as of 21 September 2026. Balbooa published no CVE, no CVSS score and no affected-version range, only a changelog line. Do not confuse it with CVE-2026-65890, which is the earlier, separate Gridbox SQL injection fixed back in 2.20.2. Cert.pl is a CNA, so a CVE may be assigned later.

Can a blind SQL injection really read my whole database?

Yes, just slowly. A time-based blind injection asks the database one true-or-false question at a time and reads the answer from how long the response takes. It is patient rather than loud, but given time it can extract usernames, email addresses, password hashes, session tokens and configuration, the same as any other SQL injection.

Do I need to assume my site was hacked?

There is no evidence this specific flaw was exploited in the wild before the fix, unlike the July mega-disclosure. Update to 2.20.3.1 first. Because the flaw can read password hashes and session tokens, it is worth checking your administrator accounts and users afterwards, which mySites.guru does automatically.

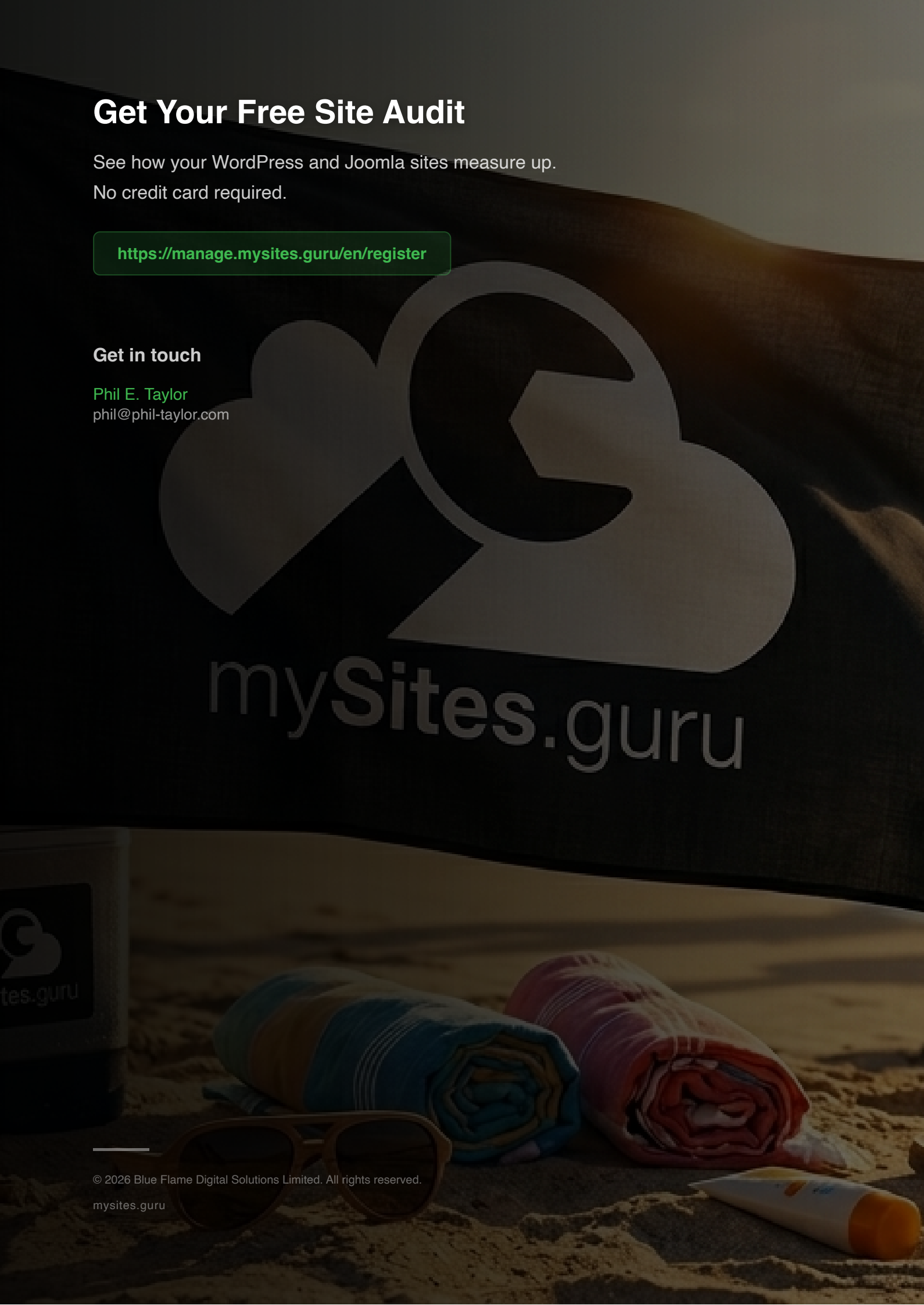
Written and edited by a human, with AI assistance. Our approach to AI

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