



Vik Booking 1.18.19 is its third security release in a week, with fixes for Vik Rent Car and Vik Rent Items

Vik Booking 1.18.19, Vik Rent Car 1.15.13 and Vik Rent Items 1.8.6 fix a CSRF gap and stored XSS. Three Vik Booking security releases in a week. What changed.

Phil E. Taylor | 26 October 2026

On 26 October 2026 E4J released Vik Booking 1.18.19 for Joomla, the third security release for the hotel booking extension in seven days, after 1.18.17 on 20 October and 1.18.18 on 21 October. The same day E4J released Vik Rent Car 1.15.13 and Vik Rent Items 1.8.6, with related fixes in their car rental and item rental code. None of that is written on the Joomla product pages, which show a version number and nothing else; the detail is in the [Vik Booking WordPress changelog](#), because E4J build the WordPress plugins from the same codebase and publish release notes only there.

So a Joomla site owner running Vik Booking has to read a WordPress changelog to learn what a Joomla update does. We did that, then compared the WordPress 1.8.18 and 1.8.19 packages to see what the notes meant in code. Two fixes stand out: the front-end information request form had no anti-CSRF token and no check that contact requests were switched on for the room, and custom-field names and links reached the booking confirmation page unescaped. Both are Medium on our assessment. The story is the cadence, not the severity.

TL;DR

- E4J released **Vik Booking 1.18.19, Vik Rent Car 1.15.13 and Vik Rent Items 1.8.6** for Joomla on 26 October 2026
- For Vik Booking it is the **third security release in seven days**: 1.18.17 (20 October, CSRF preventions), 1.18.18 (21 October, fixes from an automated security plugin review), 1.18.19 (26 October, custom-field XSS prevention)
- The front-end **information request** in Vik Booking and Vik Rent Car now checks the anti-CSRF token and rejects rooms or cars with contact requests switched off. Before, a request could be sent from another site, or for a room whose form the owner had turned off. Impact is unwanted emails, not data exposure
- **Custom-field names and popup links** on the confirmation page are now escaped in all three extensions. Exploiting the old code needs an administrator to put script into a field, so it is a low bar for damage but a high bar for access

- **No CVE** for any of it. Our CVSS 4.0 assessments are 6.9 Medium and 4.8 Medium. These are E4J's own fixes, not our find
- E4J publish **no Joomla changelog**. The release notes are on wordpress.org, and the code comments pair the version numbers
- Across the Joomla sites we manage, about **88% of the sites still flagged are on 1.18.16.1 or older**, so they have missed all three releases, not just this one

6.9

CVSS 4.0

Vik Booking and Vik Rent Car: information request with no token or access check (no CVE)

MEDIUM

mySites.guru assessment

The front-end information request task accepted a request with no anti-CSRF token and did not check whether contact requests were switched on for the room, so a request could be sent from another site or for a room whose contact form the owner had turned off. The result is unwanted information-request emails to the property; no data is exposed.

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

No login needed

Unwanted emails, no data exposure

Fixed in Vik Booking 1.18.19 and Vik Rent Car 1.15.13

▼ 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:N None: Nothing can be read

VI:L Low: Some data can be altered

VA:N None: The site stays up

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

4.8

CVSS 4.0

Vik Booking, Vik Rent Car and Vik Rent Items: stored XSS through custom fields (no CVE)

MEDIUM

mySites.guru assessment

Custom-field names and their popup-link URLs were written into the front-end booking confirmation page without escaping. An administrator, or anyone with that back-end access, could put script into a field name or link, and it would run for guests on the confirmation page.

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

Needs an administrator to set the field

Fires on the confirmation page

Fixed in all three releases

▼ 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:H High: Needs an account with elevated rights

UI:P Passive: Someone has to visit a page

What it does to the site

VC:N None: Nothing can be read

VI:N None: Nothing can be altered

VA:N None: The site stays up

What it does beyond the site

SC:L Low: Some data on other systems can be read

SI:L Low: Some data on other systems can be altered

SA:N None: Other systems stay up

What changed in Vik Booking 1.18.19

The first change is in the information request. A room page in Vik Booking has a "request information" form that emails the property, handled by a front-end task called `reqinfo`. In 1.18.19 that task checks Joomla's anti-CSRF token with `JSession::checkToken()`, and it rejects the request with a "not authorised" error when contact requests are switched off for that room. Before 1.18.19 neither check existed. A request could be posted from any other site, and it could target a room whose owner had turned the contact form off, so the switch in the back end did not stop the emails. The fix closes both, and the worst the old code allowed was unwanted information-request emails to the property. No booking or guest data was exposed through it.

The second change is the one the changelog names: "XSS prevention with custom fields management functions." On the front-end booking confirmation page, the name of each custom field and the URL of its popup link were written into the page as they were stored. 1.18.19 passes the name through `esc_html` and the link through `esc_url` before they reach the markup. Custom fields are defined by an administrator in the back end, so putting script into a field name or link takes an administrator account or someone with that access; once it is there, it runs for every guest who reaches the confirmation page. That is why the second card scores high privileges required and a Medium rather than anything louder. It is a real stored XSS and a narrow one.

Vik Rent Car 1.15.13 and Vik Rent Items 1.8.6

Vik Rent Car 1.15.13 has the same two changes. Its own `reqinfo` task, the information request for a car rather than a room, now checks the anti-CSRF token and rejects cars with contact requests switched off, and custom-field names and links are escaped on the order and car pages. The [Vik Rent Car WordPress changelog](#) lists the matching 1.4.10 release on 26 October as "XSS prevention with custom fields management functions." Rent Car has in fact had four releases in October, each listing security fixes (WordPress numbering): 1.4.7 on 8 October ("Various XSS preventions."), 1.4.8 on 13

October ("Additional XSS preventions."), 1.4.9 on 19 October ("Added multiple CSRF tokens for validation." and "Various XSS preventions."), and 1.4.10.

Vik Rent Items 1.8.6 has the custom-field escaping on its order confirmation page, and the [Vik Rent Items WordPress changelog](#) lists the matching 1.2.7 release with the same one-line note. Two smaller changes went in alongside it: an authorisation check added to a helper, and a debug switch removed. Neither is in the changelog.

What we did and did not check

We diffed the public WordPress 1.8.18 and 1.8.19 packages of Vik Booking; the Joomla packages are commercial, so the Joomla pairing comes from the code's own comments, which read "@since 1.18.19 (J) - 1.8.19 (WP)". We have not tested anything against a live site and are not publishing a working request.

Three Vik Booking security releases in seven days

Three Vik Booking security releases in seven days is the part worth noticing. 1.18.17 on 20 October listed "Multiple security improvements (CSRF preventions)." 1.18.18 on 21 October has a changelog that reads, in full, "Fixes applied for the automated security plugin review findings." 1.18.19 on 26 October added the custom-field XSS prevention. Before that run, 1.18.16 on 1 October listed "Multiple XSS preventions applied." Four releases in October with security fixes in each, and the middle one says where at least some of them come from: in its own words, "the automated security plugin review findings".

For a site owner the cadence changes what "update" means. A site that was current on 19 October is now three security releases behind. Across the Joomla sites we manage, about 9% of Vik Booking installs were already on 1.18.19 on release day. Of the sites still flagged, about 88% are on 1.18.16.1 or older, so they did not take 1.18.17 or 1.18.18 either. They have missed the whole week.

Where to find the Vik changelog when E4J publish none for Joomla

E4J's Joomla product pages on extensionsforjoomla.com show the current version number and no changelog. The release notes exist, but for the WordPress builds, which E4J produce from the same codebase and release on the same day. On 26 October that meant Vik Booking 1.8.19, Vik Rent Car 1.4.10 and Vik Rent Items 1.2.7 on wordpress.org, matching Vik Booking 1.18.19, Vik Rent Car 1.15.13 and Vik Rent Items 1.8.6 on Joomla.

The mapping is in the code rather than in any document. The source comments pair the numbers directly, as in "@since 1.18.19 (J) - 1.8.19 (WP)", so a Joomla owner who wants to know what a release fixed can open the wordpress.org changelog for the same product, find the entry dated the same day, and read that. Release notes for a paid Joomla extension should not need a detour through wordpress.org, but for these three they do.

What to do

1. Update all three. Vik Booking to 1.18.19, Vik Rent Car to 1.15.13 and Vik Rent Items to 1.8.6, on every Joomla site that runs them.
2. For Vik Booking, treat any version below 1.18.19 as behind three security releases, not one. A site on 1.18.16.1 or older has missed the CSRF fixes in 1.18.17 and the review findings in 1.18.18 as well as this release.
3. Check the custom fields in the back end. The names and popup links are the values that reached the confirmation page unescaped, so look through them for anything you did not put there.
4. If you had turned off contact requests for a room or a car, information requests for it are now rejected, including requests posted from another site. That is the setting finally doing what it says.

How mySites.guru flags these

mySites.guru added three rules to its [vulnerability database](#) on 26 October 2026: Vik Booking below 1.18.19, Vik Rent Car below 1.15.13 and Vik Rent Items below 1.8.6. Every connected Joomla site running an older version of any of them is flagged on its dashboard now, and the updates can go out across the flagged sites with the [mass updater](#). It works the same way across a [portfolio of Joomla sites](#) of any size and is part of every [subscription](#).

A burst of security releases from one vendor usually means the vendor is working through a review, and 1.18.18's note says as much by naming an automated security plugin review. In fifteen years of looking after client sites, that pattern has rarely stopped at three. The fixes so far are modest, a CSRF gap and an escaping miss, but the next one in the sequence will not announce itself any more loudly than these did, and on Joomla it will not announce itself at all. Keep these three extensions on auto-watch and expect more.

Further Reading

- [Vik Booking on wordpress.org](#) - the changelog that doubles as the release notes for the Joomla build.
- [Vik Rent Car on wordpress.org](#) - changelog for the WordPress build that pairs with Vik Rent Car 1.15.13 for Joomla.
- [Vik Rent Items on wordpress.org](#) - changelog for the WordPress build that pairs with Vik Rent Items 1.8.6 for Joomla.
- [E4J srl, extensionsforjoomla.com](#) - the vendor's Joomla product pages, version numbers only.
- [CWE-79: Improper Neutralization of Input During Web Page Generation](#) - the weakness class behind the custom-field XSS.

- CWE-352: Cross-Site Request Forgery - the weakness class behind the unchecked information request.

Frequently Asked Questions

What did Vik Booking 1.18.19 fix?

Two things. The front-end information request task now checks Joomla's anti-CSRF token and rejects requests for rooms where contact requests are switched off, and custom-field names and popup-link URLs on the booking confirmation page are now escaped before they reach the page. Neither check existed before 1.18.19.

Are Vik Rent Car and Vik Rent Items affected too?

Yes. Vik Rent Car 1.15.13, released the same day, has the same two checks on its own information request task for cars and the same custom-field escaping on its order and car pages. Vik Rent Items 1.8.6 has the custom-field escaping on its order confirmation page, plus an authorisation check on a helper and the removal of a debug switch.

Is there a CVE for the Vik Booking 1.18.19 fixes?

No. None of the fixes in Vik Booking 1.18.19, Vik Rent Car 1.15.13 or Vik Rent Items 1.8.6 has a CVE. The 6.9 Medium and 4.8 Medium scores in this post are our own CVSS 4.0 assessments, and the fixes are E4J's own work.

Why can I not find a Joomla changelog for Vik Booking?

E4J publish no changelog for the Joomla builds; the Joomla product pages show only the version number. The release notes for each Joomla version are on the [wordpress.org](https://www.wordpress.org) changelog of the matching WordPress build, which E4J release from the same codebase on the same day. Vik Booking 1.18.19 for Joomla pairs with 1.8.19 for WordPress.

How many security releases has Vik Booking had recently?

Three in seven days: 1.18.17 on 20 October 2026 with CSRF preventions, 1.18.18 on 21 October with fixes for an automated security plugin review, and 1.18.19 on 26 October with the custom-field XSS prevention. Before that, 1.18.16 on 1 October listed multiple XSS preventions.

Does mySites.guru flag outdated Vik Booking, Vik Rent Car and Vik Rent Items installs?

Yes. Since 26 October 2026 mySites.guru flags every connected Joomla site running Vik Booking below 1.18.19, Vik Rent Car below 1.15.13 or Vik Rent Items below 1.8.6 on its dashboard.

AI MODIFIED

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

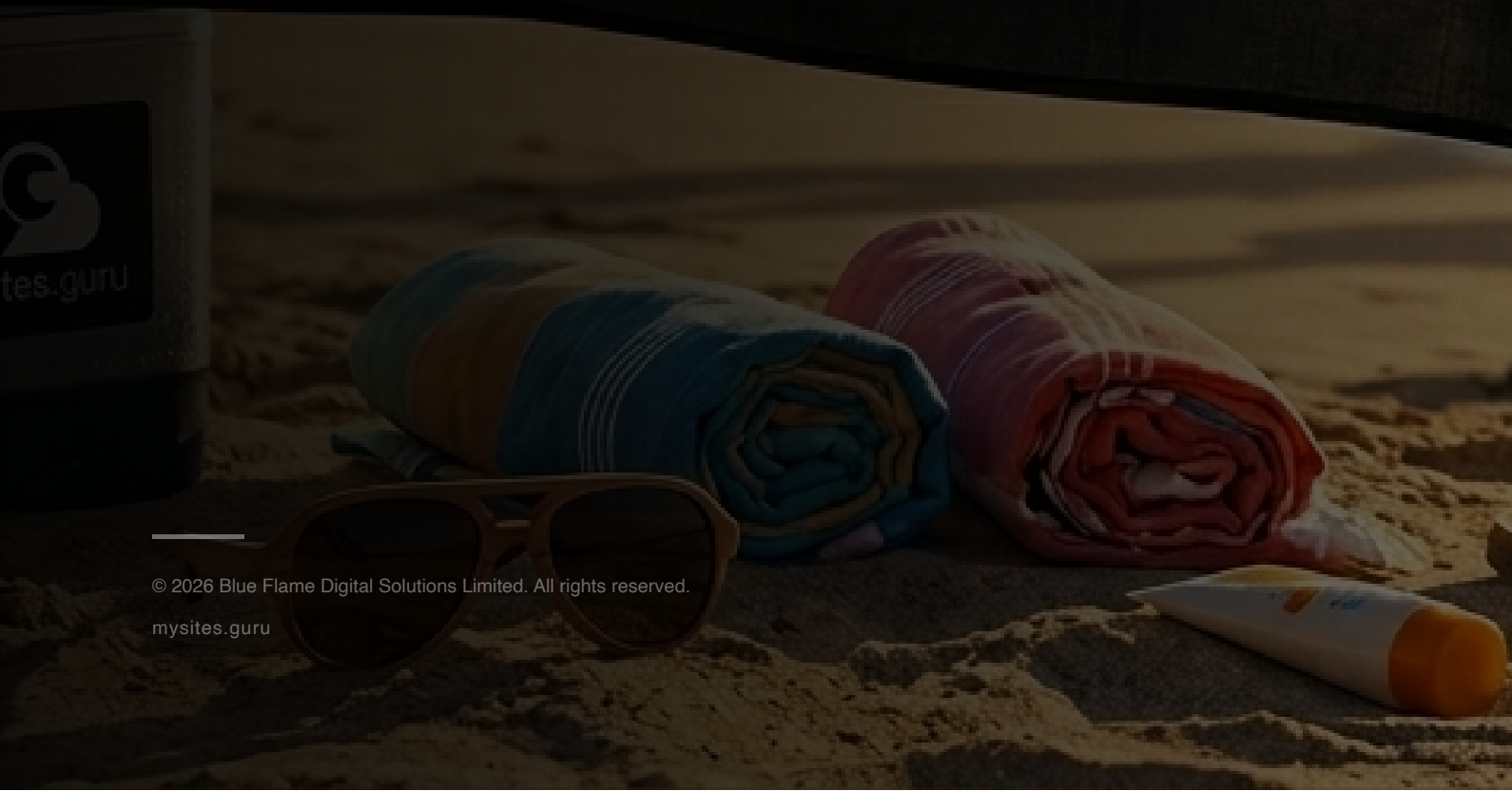
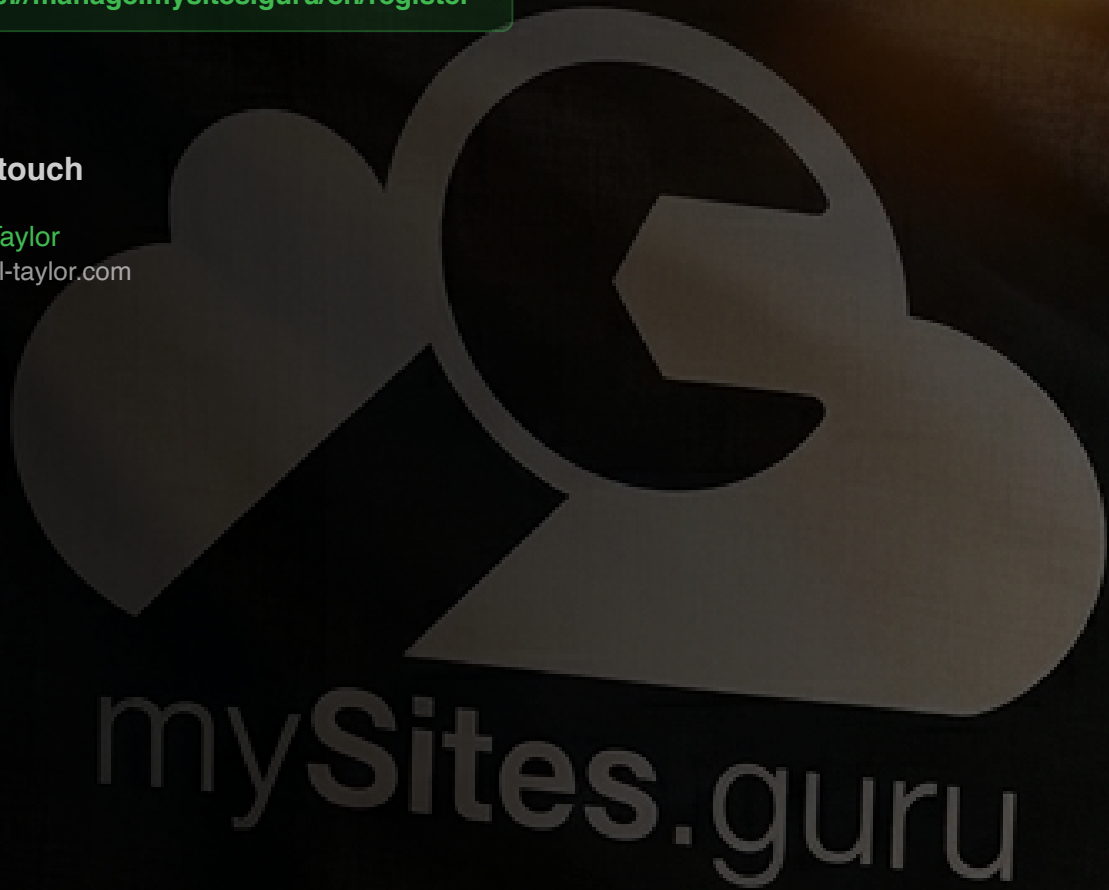
Get Your Free Site Audit

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