mySites.guru

Tassos ACF 3.1.9 for Joomla Fixes Gallery and Map Field Flaws

Tassos ACF 3.1.9 for Joomla fixes a Map field stored XSS and a Gallery image removal flaw. Update every site below 3.1.9. Not the WordPress ACF plugins.

Phil E. Taylor | 4 November 2026

TL;DR

Tassos released Advanced Custom Fields 3.1.9 for Joomla on Wednesday 4 November 2026, in Free and Pro packages, with two security fixes. The vendor's words are "Fixed a security flaw in the Gallery field's image removal" and "Fixed a security flaw in the Map field's marker labels". The Map one is a stored cross-site scripting (XSS) flaw: before 3.1.9, marker labels went out to the page unfiltered. Update every Joomla site running ACF below 3.1.9.

This is the Joomla extension by Tassos Marinos. It has nothing to do with Advanced Custom Fields for WordPress, or with the ACF Extended add-on for WordPress that has been in the vulnerability feeds all week with an unauthenticated remote code execution flaw. The two are compared below.

Not the WordPress plugin

Advanced Custom Fields for Joomla is a Tassos extension. Advanced Custom Fields for WordPress is a WP Engine plugin, and Advanced Custom Fields: Extended is a third-party add-on to it with its own CVEs this week. Same name, different CMS, different vendor, no shared code.

Joomla's ACF Is Not WordPress's ACF

Three products share the name, and this week two of them have security news. The Tassos extension is the Joomla one. The ACF Extended CVEs are the WordPress ones.

Product	CMS	Made by	This week's news	What do
Advanced Custom Fields (Tassos)	Joomla	Tassos Marinos	3.1.9 fixes Gallery and Map	Updat to 3.1

Product	CMS	Made by	This week's news	What do
			field flaws, no CVE	
Advanced Custom Fields	WordPress	WP Engine	No new CVE found this week	Keep updat as usu
Advanced Custom Fields: Extended (and PRO)	WordPress	ACF Extended (third-party add-on)	A dozen CVEs since 20 October, incl. unauthenticated RCE CVE-2026-120534 (9.8)	Updat ACF Exten to late

Scanners, news headlines and vulnerability feeds all shorten the name to "ACF", so the two get mixed up. A Joomla agency reads "ACF unauthenticated RCE" and panics; a WordPress agency reads "ACF 3.1.9 security release" and goes looking for a version that does not exist on their platform. If you run Joomla, the WordPress CVEs do not apply to you. If you run WordPress, the Tassos release does not apply to you. Agencies with both get both.

On the WordPress side, CVE-2026-120534, published on 3 November 2026 by Wordfence, is an unauthenticated remote code execution flaw in Advanced Custom Fields: Extended PRO up to 0.9.2.6, via the Dynamic Render field type, scored CVSS 3.1 9.8. Before that, on 23 October, WPScan published CVE-2026-94262 and CVE-2026-94268, unauthenticated takeover of non-administrator and administrator accounts through the front-end user update action in 0.9.2.7, fixed in 0.9.2.8, plus CVE-2026-94263, unauthenticated arbitrary shortcode execution via a form success message in 0.9.2.4 to 0.9.2.7. On 27 October Wordfence added CVE-2026-10752, unauthenticated arbitrary attachment deletion up to 0.9.2.6. Our WordPress feed holds eleven ACF Extended CVEs published between 20 and 30 October, plus the 3 November PRO one. Update ACF Extended and ACF Extended PRO to the latest

release. We covered ACF Extended's earlier 9.8 flaw, CVE-2025-13486 when it was being exploited.

The Map Field Marker Label XSS in the Joomla Extension

The Map field in ACF for Joomla lets an editor drop markers on a map, each with a label and an address. Before 3.1.9 those labels and addresses were output as saved, with no filtering. That is a stored cross-site scripting flaw: a label containing a script tag or an event handler is saved once and then runs in the browser of every visitor who views the item, and of every administrator who opens it in the back end.

Who can plant it is whoever can edit an item with a Map field on it: an article, a user profile or any other item with ACF fields. On most sites that is a content editor, which is a lower bar than Super User. Front-end editing and user profile fields push the bar lower still. The payoff for an attacker is the usual one for stored XSS, which is the session of whoever views the marker, and the administrator's session is the valuable one. We wrote up the same class of flaw in Phoca Gallery's EXIF data.

In 3.1.9, marker labels and addresses go through Joomla's InputFilter, which strips scripts and event handlers while allowing harmless HTML such as links. The change is in the Tassos Framework bundled with ACF (the system plugin "nrframework"), which moves from 6.1.39 to 6.1.51. The Map field plugin itself only changed its version headers. Tassos does not call it XSS; that is our description of what the change fixes. The Map field ships in Free and Pro, so every edition is affected.

The Gallery Field Image Removal Fix

The Gallery field ships only in ACF Pro. The vendor says 3.1.9 "Fixed a security flaw in the Gallery field's image removal" and says nothing else about it. We have not been able to read the 3.1.9 Pro package, and the vendor has not said who could trigger the flaw or what could be removed, so we will not guess.

What we can see is the shared framework code, which is in the Free package too. 3.1.9 adds a check that an image can only be removed or processed for a gallery when it is one of that gallery's stored images or the current user's own pending upload. Pending uploads now live in a temp folder scoped to the user who uploaded them. Path traversal in the image path is rejected. Together they point to old code that did not check which gallery, or whose upload, an image belonged to. How far that reached is still unknown.

The same release also fixes non-security Gallery bugs, including, in the vendor's words, "Fixed the Gallery field showing images that another user uploaded but had not saved yet", and Gallery uploads that were never saved staying in Joomla's temporary folder.

Which ACF for Joomla Versions Are Affected?

Every Advanced Custom Fields for Joomla version before 3.1.9 is affected. Tassos gives no first affected version, only that 3.1.9 is the fix, so treat anything older as needing the update. There is no CVE, no CVSS score, no researcher credit and no word on exploitation.

ACF for Joomla version	Status	What to do
3.1.9	Fixed	Nothing
3.1.1 to 3.1.8	Affected	Update to 3.1.9
2.2.0 to 3.1.0	Affected, and in range of the March framework flaw	Update to 3.1.9 and review the site
Below 2.2.0	Affected	Update to 3.1.9

Check the version on the System - ACF plugin (plg_system_acf). The individual ACF field plugins all report 1.0, whatever release you run. That catches people out when they look at the Map field plugin in particular, because the fix is in the framework and the Map field plugin only changed its version headers.

The framework is shared, and any Tassos extension can install a newer copy of it. A site that updated another Tassos extension today may already have framework 6.1.51 while

ACF itself still reads 3.1.8. Update ACF to 3.1.9 anyway, so the ACF plugins and the framework match and the site stops showing as affected.

What To Do Now

1. Update Advanced Custom Fields, Free or Pro, to 3.1.9 on every Joomla site that runs it, through Joomla's Update tab or the mySites.guru mass updater.
2. Confirm the version afterwards on the System - ACF plugin (plg_system_acf), not on the field plugins.
3. If you let anyone other than trusted staff edit items with Map fields (front-end editing, user profile fields), open the Map fields on those items and look at the marker labels and addresses for script.
4. Check administrator accounts. A stored XSS that ran in an administrator's browser can end with an account you did not create.

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 Flags ACF on Joomla and WordPress

On 4 November 2026 we added a rule that flags every connected Joomla site running Advanced Custom Fields below 3.1.9. The version is read from the ACF system plugin, plg_system_acf, for the reason above. Most ACF sites we monitor were on 3.1.8 on release day, and a small share had already updated within hours. The flag works the

same way as every other entry in our vulnerable extension list, alongside the security release flag on extension updates.

The WordPress side is covered from the same dashboard. Our WordPress vulnerability feed is imported from Wordfence, so the ACF Extended CVEs flag connected WordPress sites automatically, with no rule to write by hand. An agency running Joomla sites with Tassos ACF and WordPress sites with ACF Extended sees both lists in one place, and the mass updater pushes both updates. Every rule we hold is listed on the public vulnerabilities page, and all of this is part of the subscription.

The Last Tassos Security Release

This is the second Tassos security release this year that touches ACF. In March, CVE-2026-21627 in the Novarain/Tassos Framework was an unauthenticated file inclusion, deletion and SQL injection flaw scored CVSS 9.5, and ACF was one of the extensions bundling it. That one was fixed long ago and is a different flaw, but the pattern is the same: the framework is where the fix lives, and every Tassos extension that bundles it picks up the change. If a site skipped the March update, 3.1.9 is the moment to catch up on both.



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.

Further Reading

- Tassos: Advanced Custom Fields 3.1.9 - the vendor's own release page.
- Tassos Framework Flaw in March: CVE-2026-21627 - the earlier 9.5 Critical flaw in the framework ACF bundles.
- Ajax Endpoints: The CMS Security Blind Spot - covers ACF Extended for WordPress and its earlier CVE-2025-13486.
- CVE-2026-120534 - the ACF Extended PRO for WordPress remote code execution record.
- OWASP: Cross Site Scripting (XSS) - how stored XSS works and why output filtering stops it.

Frequently Asked Questions

What does Advanced Custom Fields 3.1.9 for Joomla fix?

Two security flaws in the Tassos Joomla extension, in the vendor's words: one in the Gallery field's image removal and one in the Map field's marker labels. The Map one is a stored cross-site scripting flaw: before 3.1.9, marker labels and addresses were output without filtering. Tassos does not use the term XSS; that is our description. The same release also fixes non-security Gallery bugs.

Is this the same as the WordPress ACF vulnerabilities this week?

No. The WordPress CVEs are in Advanced Custom Fields: Extended, a third-party add-on for WP Engine's Advanced Custom Fields plugin, and include an unauthenticated remote code execution flaw, CVE-2026-120534. The Tassos release is a Joomla extension with the same name, by a different developer, with no shared code. If you run Joomla, the WordPress CVEs do not apply to you. If you run WordPress, the Tassos release does not apply to you.

Is there a CVE for the Tassos ACF 3.1.9 fixes?

No. Tassos gives no CVE, no CVSS score, no researcher credit and no first affected version, and says nothing about exploitation. No CVE has been assigned at the time of writing.

Is Advanced Custom Fields Free for Joomla affected, or only Pro?

Both. The Map field ships in Free and Pro, so the marker label fix applies to every edition. The Gallery field ships only in ACF Pro, so the image removal fix applies to Pro sites. Both fixes are in the Tassos Framework bundled with every ACF package.

How do I check which ACF version a Joomla site runs?

Look at the version of the System - ACF plugin (plg_system_acf) in the Joomla extensions list. The individual ACF field plugins all report version 1.0, so they tell you nothing. mySites.guru reads the same system plugin version and flags any connected Joomla site below 3.1.9.



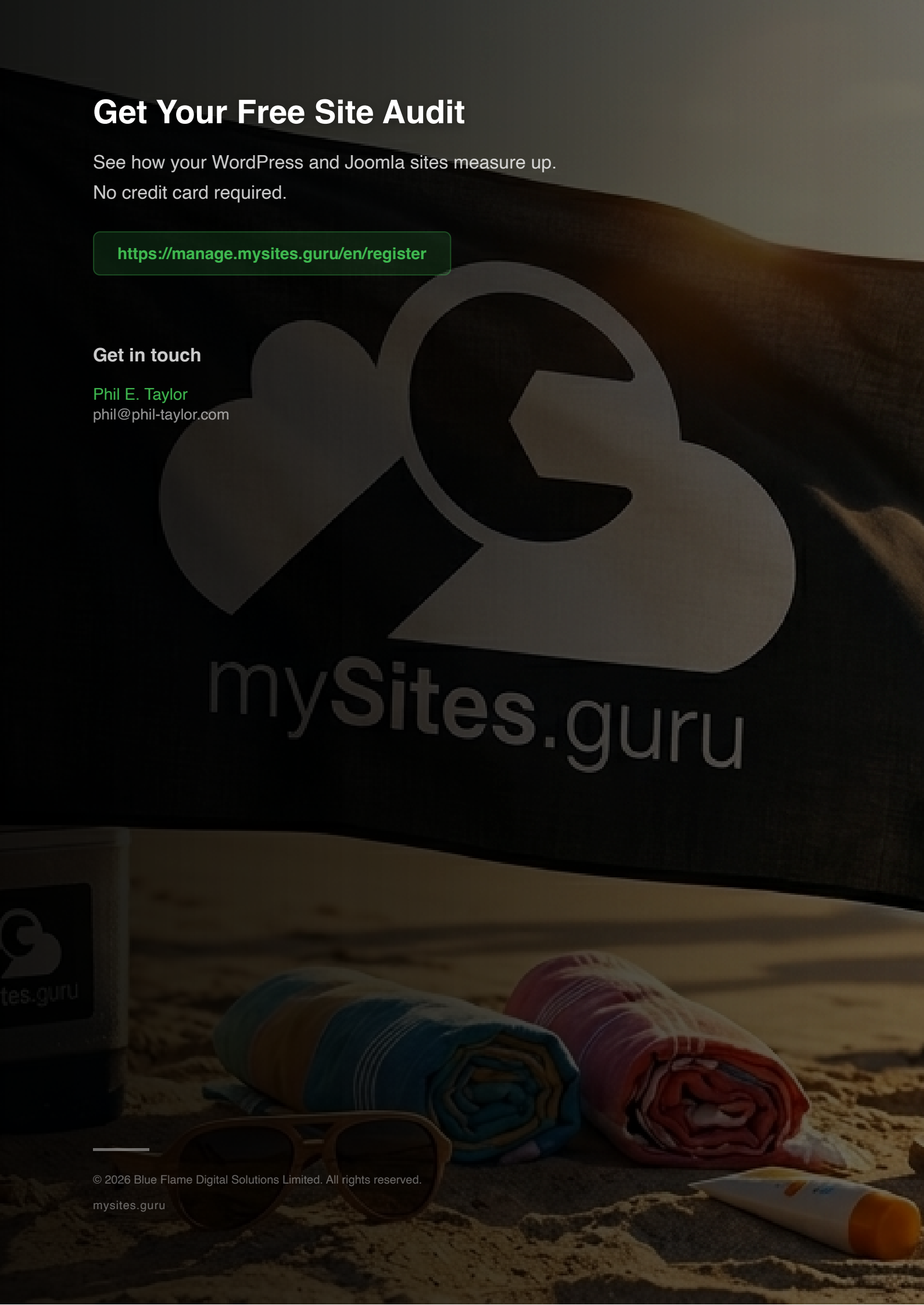
Written and edited by a human, with AI assistance. Our approach to AI

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.