mySites.guru

Avada Builder 3.15.4 Patches an Unauthenticated File Deletion Flaw (CVE-2026-8713)

Avada Builder 3.15.4 fixes a critical unauthenticated arbitrary file deletion flaw (CVE-2026-8713, CVSS 9.1) that can delete wp-config.php and hand an attacker the whole site. Here's how to find every site you manage still running an unpatched version.

Phil E. Taylor | 22 June 2026

JCE Profiles Hack · CVE-2026-48907 (22nd June): Almost 3 weeks on, the JCE hack is still being used to compromise Joomla sites, and sites that were already breached are now being trashed. Check your site today with mySites.guru.

Read the alert ›

Avada Builder, the plugin bundled with the Avada theme by ThemeFusion, runs on around 1 million WordPress sites. On 19 June 2026 a new CVE landed against it: CVE-2026-8713, an unauthenticated arbitrary file deletion flaw rated **CVSS 9.1 Critical**. The fix shipped quietly weeks earlier in version **3.15.4**, released on 2 June 2026.

This is a more dangerous bug than the file read and SQL injection pair we covered in 3.15.3. Those leaked data. This one deletes it. An unauthenticated attacker can submit a crafted payload through a public Avada form and delete any file on the server, and deleting the right file turns into a full site takeover. Update to **3.15.4** now.

If you manage WordPress sites for clients, the advisory is the easy bit. The work is figuring out which of your sites are still on 3.15.3 or earlier, then pushing the update to every one of them. Across the mySites.guru network we track Avada Builder on nearly 1,000 sites belonging to hundreds of agencies, and when we checked our own connected sites against this CVE, every single Avada Builder install we monitor was on a version below the 3.15.4 fix. Nobody had updated yet. That gap is the whole point of this post.

Finding Every Avada Builder Site in Your Portfolio

Up to about ten sites, you can log in to each one and check the Plugins screen. Past that, you need a single view. The Plugins screen approach is slow, error-prone, and only tells you what was on disk the last time someone looked.

mySites.guru's WordPress Extensions inventory tracks every installed plugin across every connected site, refreshed on each snapshot. Search for "Avada Builder" (or the slug `fusion-builder`) and you get every version across your portfolio, grouped by

version number, with a “Which sites?” button that lists exactly where each version is running.

mySites.guru subscribers: find every Avada Builder install across your sites

Open Avada Builder Extension Search

Lists every version of Avada Builder across your connected sites. Anything on 3.15.3 or earlier needs the 3.15.4 patch. Not a subscriber? Sign up free and connect your sites.

The same inventory feeds the vulnerability scanner. mySites.guru cross-references every installed plugin against the Wordfence Vulnerability API twice a day, so when a CVE like CVE-2026-8713 drops, sites running affected versions get flagged with a red warning banner. No security feeds to watch.

Bulk Updating Avada Builder Across Hundreds of Sites

Once you know which sites need updating, the mass updater handles the rollout. Tick the sites that need 3.15.4, push the update across all of them from one screen. The same workflow covers any plugin, theme, or core update, so the routine you wire up once works for every future CVE. Pair it with the Akeeba Backup or All-In-One Migration integration to back up each selected site first.

With a file deletion flaw the backup-first habit earns its keep twice over. If a site was hit before you patched, the missing file is the damage, and a recent backup is your fastest route to a working site.

For agencies managing 50+ WordPress sites

Avada Builder ships with the Avada theme, so most clients running Avada have this plugin whether they know it or not. The patch is the easy bit; the inventory is the work. See how bulk updates work in mySites.guru.

If the patch needs more than a quick test on a particular site, deactivating Avada Builder takes the vulnerable form handler out of play while you schedule a maintenance

window. Alternatively, removing or unpublishing any public Avada form that stores entries to the database closes the precondition the attack needs.

CVE-2026-8713: Unauthenticated Arbitrary File Deletion

Detail	Value
CVE	CVE-2026-8713
CVSS	9.1 Critical (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H`)
Type	Unauthenticated Arbitrary File Deletion (Path Traversal, CWE-22)
Affected versions	All versions up to and including 3.15.3
Patched version	**3.15.4** (Avada 7.15.4, 2 June 2026)
Auth required	No
Precondition	A public Avada form that stores entries in the database
Bounty	$3,600.00
Researcher	daroo (via Wordfence Bug Bounty)

The flaw lives in `maybe_delete_files()` in the `Fusion_Form_DB_Entries` class. When Avada cleans up old form entries, it works out which uploaded files belong to an entry and deletes them. It builds those file paths by string-replacing the uploads URL, with no `realpath()` resolution and no check that the final path stays inside the uploads directory.

That means `../` traversal sequences in submitted form data survive into the deletion path. The handler is registered as a `nopriv` AJAX action, so it answers anonymous requests, and an attacker can drive the privacy-cleanup mechanism by controlling the expiration fields on the form submission. Put those together and an unauthenticated visitor can submit something like:

```
wp-content/uploads/fusion-forms/../../../wp-config.php
```

and have the cleanup routine delete `wp-config.php` for them.

Why deleting a file is as bad as uploading one

A deletion primitive sounds less alarming than file upload or code execution. It is not, because of one specific target.

`wp-config.php` holds the database credentials WordPress needs to boot. Delete it and WordPress can no longer connect to its database, so on the next request it assumes this is a fresh install and serves the setup wizard. An attacker who triggered the deletion can now walk through that wizard, point the install at a database they control, and end up with an administrator account on your domain. From an admin account, dropping a malicious plugin and running arbitrary PHP is routine.

So the chain runs from an unauthenticated request to a deleted config file, to a forced reinstall the attacker drives, to an administrator account and arbitrary code. The first step needs no login and no user interaction, which is why the score is 9.1 and not something lower.

This is the same lesson as the AJAX endpoints blind spot we have written about before: a `nopriv` handler is open to the entire internet, so every input it touches has to be treated as hostile. A single path-containment check in `maybe_delete_files()` would have stopped this.

Is it being exploited yet?

As of 22 June 2026, no security vendor has published evidence of in-the-wild exploitation, indicators of compromise, or attack telemetry for CVE-2026-8713. The Wordfence advisory describes the mechanism and the impact, not an active campaign.

That is good news with a short shelf life. The flaw is unauthenticated and the payload path is no secret now the CVE is public, and a critical, public CVE against a million-

install plugin is exactly what the mass scanners go looking for. Patching ahead of that is cheap right now. It usually does not stay cheap for long.

How do I watch for exploitation after patching?

Patching closes the door. Monitoring tells you whether anyone walked through it first. With a file deletion flaw the tell is on the filesystem.

mySites.guru's real-time alerting covers the signals that matter after a destructive CVE:

- Missing or changed core, theme, and plugin files. If `wp-config.php` was deleted and recreated, or new PHP files appeared in `wp-content/`, the file-change alert fires before the next snapshot.
- New administrator accounts. Anything created at admin level fires an alert, whether it came in through the setup wizard, the REST API, or directly through the database.
- wp-admin login activity, with IP, user agent, and timestamp. An unfamiliar admin login on a site that should have no new admins is the cheapest tell that the takeover chain ran.

If any of those fire, the malware scanner and the WordPress hacked recovery workflow handle the remediation.

How to verify your sites are patched

Three checks, in order of speed:

1. **mySites.guru**: open the Avada Builder extension search and confirm every install is on 3.15.4 or later. Anything on 3.15.3 or earlier still needs updating.
2. **WP-CLI** on a single site: `wp plugin get fusion-builder --field=version`
3. **wp-admin**: Plugins page, find Avada Builder in the list, check the version.

If WordPress reports no update available, check that the Avada theme is registered with a current ThemeFusion licence. Avada Builder updates come through ThemeFusion's update channel, not the WordPress.org directory, so a lapsed licence leaves the plugin pinned to an old version.

What to do if you suspect a site was hit

Because the damage is a deleted file, the symptoms are loud: a site that suddenly shows the WordPress setup screen, a fatal "error establishing a database connection", or missing media and uploads. If you see those on an Avada site that was on 3.15.3 or earlier, treat it as a possible exploitation, not a random outage.

1. Restore from a known-good backup

If `wp-config.php` or other files were deleted, the fastest clean recovery is a restore from before the deletion. This is where the one-click backup of files and database pays off. A mySites.guru snapshot records config and version state, but it is not a restorable backup, so for a rollback you want the full backup.

Restore, then immediately update to 3.15.4 so the same payload cannot delete the file again.

2. Hunt for rogue admin accounts

If the deletion forced a reinstall and an attacker walked through the setup wizard, they could now hold an administrator account. Check the user table:

```
SELECT ID, user_login, user_registered, user_email
FROM wp_users
ORDER BY user_registered DESC
LIMIT 20;
```

Anything created since 2 June 2026 that you do not recognise is suspect.

How mySites.guru helps: universal user management sorts every account across every connected site by registration date, so you can scan hundreds of sites for new admins in one screen rather than logging into each wp-admin.

3. Look for backdoors and modified files

A reinstall under attacker control is a perfect moment to plant persistence. Look for unexpected PHP files in `wp-content/uploads/`, `wp-content/mu-plugins/`, and anywhere else uploads should not contain executable code.

```
find wp-content/uploads -name '*.php' -type f
find wp-content/mu-plugins -name '*.php' -mtime -30
```

How mySites.guru helps: the suspect content scanner runs the same pattern matching across every connected site. Anything it flags gets a one-click AI-powered malware analysis that explains what the code does in plain English, and the hidden files report flags orphan PHP files outside the normal core, theme, and plugin paths.

A note on 3.15.5

Avada shipped another security release, **3.15.5** (Avada 7.15.5), on 15 June 2026. It fixes a *separate* arbitrary file deletion bug that occurs when deleting custom icon sets, plus a couple of other issues. That is not the same flaw as CVE-2026-8713, which is fixed in 3.15.4 and lives in the form handler.

The practical takeaway is simple: do not stop at 3.15.4. Update to the latest Avada release available to you so you pick up both file deletion fixes at once. If your extension inventory shows sites on 3.15.4, they have the CVE-2026-8713 fix but not the icon-set fix, so push them on to the current version.

Further Reading

- Wordfence advisory for CVE-2026-8713 - the original disclosure with the technical detail
- Avada 7.15.4 security update notes - ThemeFusion's own release announcement
- CVE-2026-8713 record - the canonical CVE entry
- Avada Builder Patches Two Security Issues in 3.15.3 - the earlier file read and SQL injection pair in the same plugin

Frequently Asked Questions

What is CVE-2026-8713 in Avada Builder?

CVE-2026-8713 is an unauthenticated arbitrary file deletion vulnerability in Avada Builder versions up to and including 3.15.3. A flaw in the maybe_delete_files() function fails to validate file paths, so an attacker can submit a path-traversal payload through a public Avada form and delete any file on the server, including wp-config.php. It is rated CVSS 9.1 Critical and fixed in version 3.15.4.

Which Avada Builder versions are affected by CVE-2026-8713?

All Avada Builder versions up to and including 3.15.3 are vulnerable. The fix shipped in version 3.15.4 (Avada theme 7.15.4), released on 2 June 2026. If your site runs 3.15.3 or earlier, it needs the update. The Avada theme uses version numbers in the 7.15.x range while the bundled Builder plugin uses 3.15.x, so 7.15.4 and 3.15.4 are the same release.

Does CVE-2026-8713 need a login to exploit?

No. The flaw is unauthenticated. The vulnerable code sits behind a nopriv AJAX handler that anonymous visitors can reach, so an attacker needs no account on the site. The one precondition is a publicly accessible Avada form configured to store its entries in the database.

How can deleting a file lead to a full site takeover?

If an attacker deletes wp-config.php, WordPress no longer has database credentials and drops back into its installation wizard. From there an attacker can point the install at a database they control, which lets them create an administrator account and run arbitrary PHP. Arbitrary file deletion of the right file becomes full remote code execution and site takeover.

How do I find every WordPress site I manage that runs a vulnerable Avada Builder?

Manually you would log in to each site and check the Plugins page. With mySites.guru you open the WordPress Extensions inventory, filter for Avada Builder (slug fusion-builder), and click 'Which sites?' to list every connected site running the plugin with its installed version. Anything on 3.15.3 or earlier needs the 3.15.4 patch, and you see them all on one screen.

Is CVE-2026-8713 being exploited in the wild?

As of 22 June 2026 there is no confirmed evidence of in-the-wild exploitation. The flaw is critical and straightforward to exploit once a vulnerable site is found, which is why patching

promptly matters, but no security vendor has published attack telemetry or indicators of compromise yet. Treat it as a patch-now flaw rather than an active incident.

Why might WordPress show no update available for Avada Builder?

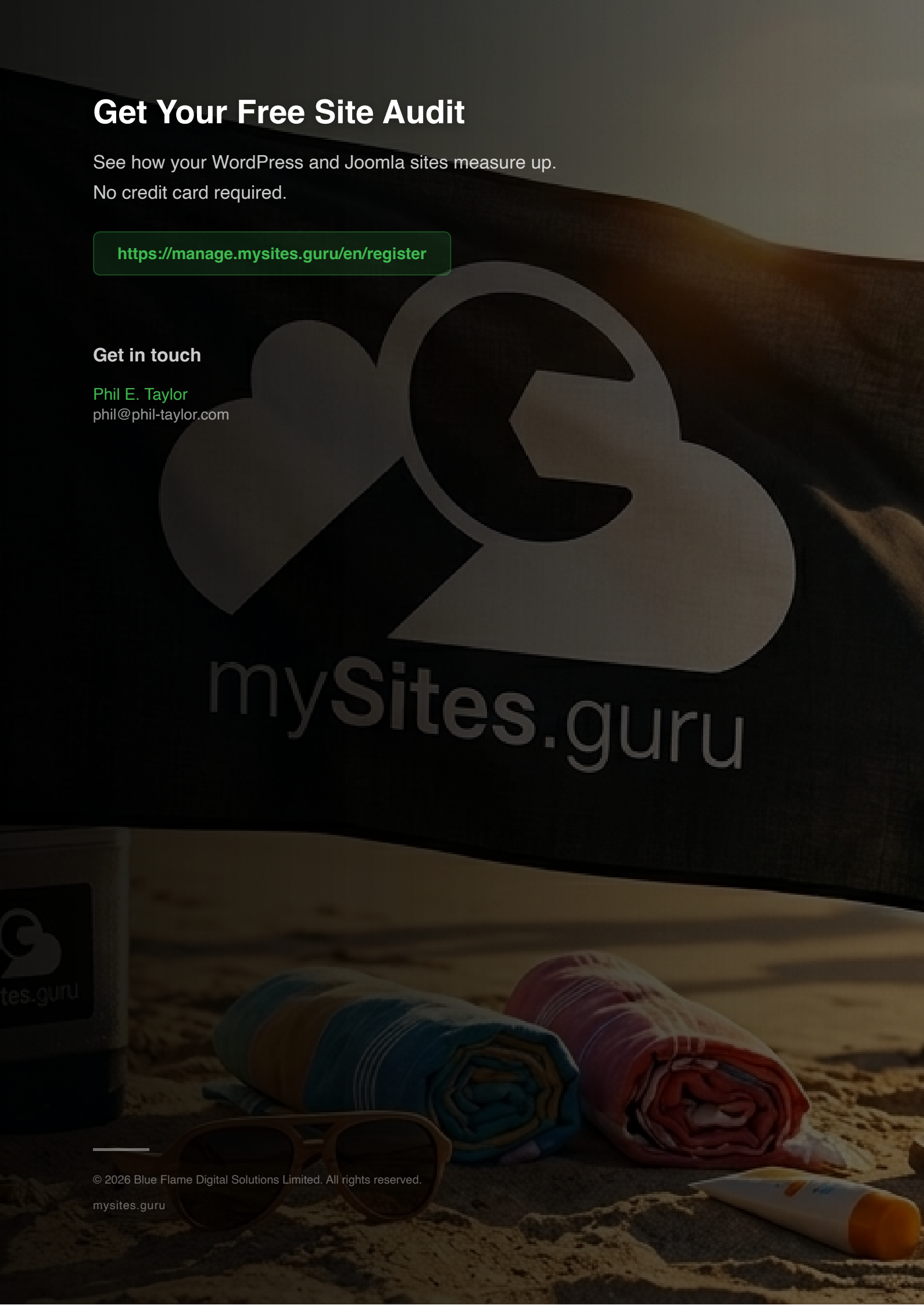
Avada Builder updates come through ThemeFusion's own update channel, not the WordPress.org plugin directory. If the Avada theme licence has lapsed or was never registered on that site, the plugin stays pinned to its installed version and shows no update. Register a current ThemeFusion licence and the 3.15.4 update will appear.

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