contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

themefic Ultra Addons for Contact Form 7: new CVE

CVE-2026-102435 · record published 2 November 2026

Analysis Report

WordPress sites with Ultra Addons for Contact Form 7 on version 3.5.54 or earlier and the PDF Generator add-on active need to act. Check whether PDF Generator is enabled — if it is, disable it …

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/themefic-ultra-addons-for-contact-form-7-cve-2026-102435

Correction, 5 November 2026: an earlier version of this note described the last affected version as the first version that is not affected. The CVE record lists 3.5.54 as affected.

The bottom line

> *WordPress sites with Ultra Addons for Contact Form 7 on version 3.5.54 or earlier and the PDF Generator add-on active need to act. Check whether PDF Generator is enabled — if it is, disable it immediately and update the plugin; if it is not, your risk is significantly lower.*

At a glance

Fact	Detail
Product	themefic Ultra Addons for Contact Form 7 (CVE-2026-102435)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by Wordfence on 2 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 5 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No fixed version in the record. The 3.5.55 changelog (11 October 2026) says Wordfence-reported issues were resolved; 3.5.57 (1 November 2026) adds PDF filename sanitisation. Neither names this CVE.
Who looks first	WordPress site owners and administrators running Ultra Addons for Contact Form 7 (by themefic) on version 3.5.54 or earlier, where the PDF Generator add-on is active and at least one Contact Form 7 form is configured for PDF generation.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run the Ultra Addons for Contact Form 7 plugin on any WordPress site?	Nothing to do for this CVE.	Check the version (next question).
Is the installed version 3.5.54 or earlier?	The record does not list your version as affected. Monitor for a confirmed fix statement.	Check whether PDF Generator is enabled (next question).
Is the PDF Generator add-on enabled in the plugin settings?	The record says this CVE cannot be exploited without it. Update the plugin when able.	Check whether a CF7 form is configured for PDF generation (next question).

Is at least one Contact Form 7 form configured to generate a PDF?	Exploitation also requires a configured form; risk is lower. Update when able.	Disable PDF Generator immediately and update the plugin.

What it is

An unauthenticated attacker can delete any file on the server. Deleting a critical file such as wp-config.php can then allow the attacker to run arbitrary code, taking full control of the site.

Why it matters

A score of 9.8 reflects that no login is required. The record says the flaw uses a PHP deserialization gadget chain (CWE-502) triggered through a Contact Form 7 submission object's destructor, enabling arbitrary file deletion. Our reading is that this makes the attack reliable: deleting wp-config.php forces WordPress into a reinstall state, giving the attacker the chance to set new credentials and take over the site. The two conditions — PDF Generator enabled and a form configured — narrow the exposed population, but both are normal for a site using this plugin's advertised feature.

What the vendor's advisory says

We read two pages on plugins.svn.wordpress.org and wordpress.org. In short:

- The changelog for 3.5.55 (11 October 2026) states: 'Issues reported by Wordfence have been resolved. Enhanced overall plugin security.' It does not name CVE-2026-102435.
- The changelog for 3.5.57 (1 November 2026) states: 'PDF filename sanitisation and secure mPDF content handling.' It does not name this CVE.
- The changelog for 3.5.56 (27 October 2026) states: 'Enhanced overall plugin security.' It does not name this CVE.

Things people will get wrong

- Every site with this plugin is at risk. The record states exploitation requires PDF Generator to be active and at least one CF7 form configured for PDF generation. Sites without those conditions are not in the affected path.
- Updating to 3.5.57 confirms you are safe. The 3.5.57 changelog mentions PDF filename sanitisation but does not name CVE-2026-102435. The CVE record names no fixed version; seek written confirmation from the vendor.
- This is a file-deletion flaw only, not a code-execution risk. The record says deleting the right file — the example given is wp-config.php — can easily lead to remote code execution. File deletion is the method; full site takeover is the stated impact.

How we would triage it

This is our judgement.

Step 1: Find the plugin version you run

- In the WordPress admin, go to Plugins and find 'Ultra Addons for Contact Form 7'. The version number appears beneath the plugin name.
- The affected range is all versions up to and including 3.5.54, as stated in the record.

Step 2: Check whether PDF Generator is enabled

- In the WordPress admin, open the Ultra Addons settings and look for the PDF Generator section. The record states this CVE can only be exploited when this feature is enabled.
- Also check each Contact Form 7 form for a PDF Generator tab; exploitation requires at least one form configured for PDF generation.

Step 3: Disable PDF Generator if on an affected version

- If you are on version 3.5.54 or earlier and PDF Generator is active, turn it off in the plugin settings until the plugin is updated.
- The record says the attack requires this feature to be active; disabling it removes the exploitable condition while you arrange the update.

Step 4: Update the plugin and confirm the fix

- Update to the latest available version. The 3.5.55 changelog (11 October 2026) says Wordfence-reported issues were resolved; 3.5.57 (1 November 2026) adds PDF sanitisation. Neither names this CVE.
- Ask your IT provider or the plugin vendor for written confirmation that the installed version addresses CVE-2026-102435 before re-enabling the PDF Generator.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are reviewing CVE-2026-102435, a score-9.8 flaw in the Ultra Addons for Contact Form 7 WordPress plugin (by themefic), affecting versions up to and including 3.5.54. An unauthenticated attacker can delete arbitrary server files; the record says this can lead to remote code execution. The flaw is only exploitable when the PDF Generator add-on is active and at least one Contact Form 7 form is configured for PDF generation. Please confirm: (1) whether we run this plugin, (2) the version installed, (3) whether PDF Generator is enabled, and (4) whether the installed version addresses this CVE. The CVE record names no confirmed fixed version. Please provide written confirmation of the version and fix status by 12 November 2026.*

The weakness behind it

The record classes this as CWE-502.

The sources, in their words

The CVE record:

> *The Ultra Addons for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the _getObjAttr function in all versions up to, and including, 3.5.54. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). This requires the PDF Generator add-on to be active and a Contact Form 7 form to be configured for PDF generation, as the WPCF7_Submission POP gadget chain relies on CF7 being present to complete the file deletion via __destruct(). Note: This vulnerability can only be exploited when the ...*

Versions of themefic Ultra Addons for Contact Form 7 the record lists as affected:

- all versions up to and including 3.5.54

The record gives no version ranges. Use the vendor's advisory for the affected versions.

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-102435
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-102435
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The CVE record names no confirmed fixed version. Neither the 3.5.55 nor the 3.5.57 changelog entry names CVE-2026-102435.
- It is not stated whether the PDF Generator feature is enabled by default on installation or must be explicitly activated.
- The record does not say whether a specific server configuration or WordPress multisite setup changes the exposure.
- No temporary workaround other than disabling the PDF Generator feature is described in the available sources.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 5 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-102435: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
2 November 2026	CVE record published by Wordfence.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Plugin on version 3.5.54 or earlier, PDF Generator enabled, a CF7 form configured, site internet-facing	High	Immediately — disable PDF Generator today, update as soon as possible
Plugin on version 3.5.54 or earlier, PDF Generator enabled, a CF7 form configured, intranet only	High	This week — the attack needs no login; score is 9.8
Plugin on version 3.5.54 or earlier, PDF Generator not enabled or no CF7 form configured for PDF	Medium	Next patch cycle — feature must be active per the record
Plugin on version 3.5.55 to 3.5.57, no confirmed fix statement for this CVE in the record	Low	Seek vendor confirmation; update to 3.5.57 if not already there

Plugin not installed on any site	None	Nothing to do for this CVE

Appendix 4. Definition of done

- Every themefic Ultra Addons for Contact Form 7 you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-102435: https://www.cve.org/CVERecord?id=CVE-2026-102435
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: plugins.svn.wordpress.org/ultimate-addons-for-contact-form-7/tags/3.5.52/: https://plugins.svn.wordpress.org/ultimate-addons-for-contact-form-7/tags/3.5.52/addons/pdf-generator/pdf-generator.php
- Advisory or release notes read: wordpress.org/plugins/ultimate-addons-for-contact-form-7/: https://wordpress.org/plugins/ultimate-addons-for-contact-form-7/
- Reference in the CVE record: www.wordfence.com: https://www.wordfence.com/threat-intel/vulnerabilities/id/187777a4-3438-489c-ad3b-7e16753189d6?source=cve
- Reference in the CVE record: plugins.trac.wordpress.org: https://plugins.trac.wordpress.org/changeset/3738548/ultimate-addons-for-contact-form-7