

SECURITY ADVISORY

addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder: new CVE

CVE-2026-109220 · record published 31 October 2026

Analysis Report

PREPARED BY	NamiQ	DATE	31 October 2026
FACTS AS OF	31 October 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/addonsorg-pdf-invoice-for-woocommerce-drag-cve-2026-109220

The bottom line

If you run a WordPress shop with WooCommerce and this invoice plugin, act today: the record says no login is needed to attack it. First find out whether the plugin is installed and which version. If you do not use it, you can stop reading.

At a glance

Fact	Detail
Product	addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder (CVE-2026-109220)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by Wordfence on 31 October 2026. Not on CISA's list of exploited vulnerabilities when we read it on 31 October 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Anyone running a WordPress shop with WooCommerce and the PDF Invoice for WooCommerce plugin. The record names shops that take Direct Bank Transfer or cheque payments as a way in on a default install.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run WordPress with WooCommerce and the PDF Invoice for WooCommerce plugin?	Nothing to do for this CVE.	Check the plugin version (next question).
Is the plugin on a version the record lists as affected?	Keep the version and note it down.	Treat the shop as exposed and go to the next question.
Can visitors reach your shop checkout from the internet?	Lower risk, but still update at the next opportunity.	Act now: reduce exposure, then update.
Do you offer Direct Bank Transfer or cheque payment at checkout?	The record's described route does not apply as written. Update anyway.	This is the route the record describes. Treat it as urgent.

What it is

The record says the plugin passes text from the checkout note field into code that rebuilds PHP objects without checking it. Someone with no account can place an order through the public checkout and run code on the server.

Why it matters

Our reading is that code execution on a shop server gives an attacker the orders, customer details and files the site can reach, and a base for further access. The record says a default install is reachable through an ordinary checkout, so no special setup protects you. A score of 9.8 with no login needed is reason enough to act before anyone exploits it.

Things people will get wrong

- "It is not on CISA's list, so we can wait." The record is new. Not being listed yet says nothing about whether anyone is attacking it. The record says no login is needed.
- "Only customers who have accounts can reach it." The record says an unauthenticated attacker can place an anonymous checkout through the public interface.
- "We only use card payments, so we are safe." The record describes bank transfer or cheque as the route that triggers the code path. It does not say other methods are safe, so check before relying on that.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- List the active plugins on each WordPress site and note the version of this invoice plugin.
- Check staging and test copies too. They often hold the same plugin and face the internet.

Step 2: Reduce exposure while you wait

- If you cannot update at once, deactivate the plugin. The record says the flaw sits in the invoice code path, so a deactivated plugin removes it.
- Ask your host or provider whether they can block anonymous orders until the plugin is dealt with.

Step 3: Update or remove the plugin

- The record does not name a fixed version, and its range and description disagree about 7.1.1. Ask the vendor or your provider which release is fixed.
- If no fixed release is confirmed, keep the plugin off and use another way to produce invoices.

Step 4: Check afterwards

- Confirm the installed version in writing and that the plugin is updated, or off.
- Review recent orders for odd text in the customer note field.

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.

Hello, we need to check our exposure to CVE-2026-109220, a flaw in the PDF Invoice for WooCommerce + Drag and Drop Template Builder plugin for WordPress. Please tell us whether any of our sites run it, on which hosts, and which version. The record says no login is needed to exploit it. It does not name a fixed version, so please confirm with the vendor which release is fixed. If we cannot update straight away, please deactivate the plugin. Please confirm the version and the fix to us in writing by the end of this week.

The weakness behind it

The record classes this as CWE-502.

The sources, in their words

The CVE record:

The PDF Invoice for WooCommerce + Drag and Drop Template Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 7.1.1 via the 'customer_note' parameter parameter. This is due to insufficient sanitization of the customer_note checkout field, which is inlined verbatim into invoice HTML, entity-decoded back into a live tag by simplehtmldom, reassembled into raw bytes by mPDF, and passed to unserialize() in _getObjAttr without validation. This makes it possible for unauthenticated attackers to execute code on the server. An unauthenticated attacker can trigger the vulnerable code path on a default install by placing an anonymous WooCommerce ...

Versions of addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder the record lists as affected:

- all versions up to, but not including, 7.1.1

What we do not know yet

- Which release is fixed: the record's range and its description disagree about whether 7.1.1 is affected.
- Whether the vendor has published an advisory or any workaround. No vendor page could be read.
- Whether any attacker is using this. The record says nothing about it.
- Whether payment methods other than bank transfer or cheque can reach the same code.
- 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 31 October 2026. We have not read the vendor's advisory page and we have not tested it.
- 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-2026-109220: 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
31 October 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
Shop facing the internet, plugin active, bank transfer or cheque payment offered	High	today
Shop facing the internet, plugin active, other payment methods only	High	this week, after checking the route
Plugin installed but deactivated	Low	next patch cycle; consider removing it
Staging or test copy of the shop reachable from the internet	Medium	this week
No WordPress, or the plugin is not installed	None	none for this CVE

Appendix 4. Definition of done

- Every addonsorg PDF Invoice for WooCommerce + Drag and Drop Template Builder 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-2026-109220: <https://www.cve.org/CVERecord?id=CVE-2026-109220>
- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Reference in the CVE record: www.wordfence.com: <https://www.wordfence.com/threat-intel/vulnerabilities/id/1bc3529c-6161-4b89-8a35-c3a9b7b8c308?source=cve>
- Reference in the CVE record: plugins.trac.wordpress.org: <https://plugins.trac.wordpress.org/browser/pdf-for-woocommerce/tags/7.1.1/vendor/mpdf/mpdf/src/Mpdf.php#L9105>
- Reference in the CVE record: plugins.trac.wordpress.org: <https://plugins.trac.wordpress.org/browser/pdf-for-woocommerce/tags/7.1.1/woocommerce/shortcodes.php#L708>