contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Barn2 Plugins Document Library Pro: new CVE

CVE-2026-122662 · record published 15 November 2026

Analysis Report

If any of your WordPress sites runs Document Library Pro, update the plugin to 4.2.2 or later this week. First find out whether any site uses it; if none does, you can stop reading.

PREPARED BY	NamiQ	DATE	16 November 2026
FACTS AS OF	16 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/barn2-plugins-document-library-pro-cve-2026-122662

The bottom line

> *If any of your WordPress sites runs Document Library Pro, update the plugin to 4.2.2 or later this week. First find out whether any site uses it; if none does, you can stop reading.*

At a glance

Fact	Detail
Product	Barn2 Plugins Document Library Pro (CVE-2026-122662)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by Patchstack on 15 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 16 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	4.2.2 (Patchstack's advisory names it as the patched version; the CVE record says to update to at least 4.2.2)
Who looks first	Anyone running WordPress with the Barn2 Plugins Document Library Pro plugin (document-library-pro) on a version before 4.2.2. Check first any site that anyone on the internet can reach.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run WordPress with the Document Library Pro plugin installed?	Nothing to do for this CVE.	Check the plugin version (next question).
Is the installed plugin version earlier than 4.2.2?	You are on the fixed release or later. Keep a note of the version.	Treat the site as exposed and update it.
Can anyone outside your organisation reach the site?	Lower urgency, but still update at the next patch cycle.	Update now; the advisory says no login is needed.

What it is

The record says the plugin deserialises untrusted data, which allows object injection. Patchstack's advisory says no login is needed and that an attacker can make the site run harmful actions on the server.

Why it matters

Our reading is that this is worth acting on before anyone is seen using it. Patchstack's advisory gives it a score of 9.8, needs no login, and says flaws like this are used in mass campaigns against many sites regardless of their size. A WordPress plugin sits on the public web, so a small firm's site is as reachable as any other.

What the vendor's advisory says

We read one page on patchstack.com. In short:

- Patchstack's advisory says versions before 4.2.2 are vulnerable and 4.2.2 is the patched version.
- It rates the flaw high priority with a score of 9.8 and says the required privilege is unauthenticated.
- It says the flaw is expected to become exploited and is the kind used in mass-exploit campaigns.
- It says to update the plugin at once, and to ask your hosting provider or web developer for help if you cannot.
- It says the issue was reported on 13 October 2026 and published on 13 November 2026.

Things people will get wrong

- "It is not on the CISA list, so it is not urgent." The record is new. The advisory says the flaw is expected to be exploited and needs no login, so waiting for a listing costs time.
- "Our site is small, so nobody will bother." The advisory says attacks of this kind hit thousands of sites at once, regardless of traffic size or popularity.
- "A deactivated plugin is safe." The sources do not say whether a deactivated plugin is exposed. Update or remove it rather than assume.

How we would triage it

This is our judgement.

Step 1: Find the sites and plugin versions you run

- List every WordPress site you or your provider manage, including test and old sites.
- Check each for the plugin document-library-pro and note its version and whether it is active.

Step 2: Reduce exposure while you arrange the update

- If you cannot update at once, ask your hosting provider or web developer for help, as the advisory suggests.
- Consider switching the plugin off on public sites until it is updated, if the site can work without it.

Step 3: Update to 4.2.2 or later

- Take a backup, then update the plugin to 4.2.2 or later, the version the advisory names as patched.
- Test that the document pages still load.

Step 4: Confirm the result

- Check that each site now reports 4.2.2 or later.
- Ask your provider for written confirmation of the version on every site.

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 confirm our exposure to CVE-2026-122662 in the WordPress plugin Document Library Pro by Barn2 Plugins. Please tell us whether any site we run uses it, where, and which version. The CVE record and the vendor advisory say versions before 4.2.2 are affected and 4.2.2 is the fixed version. Please update any affected site to 4.2.2 or later and send us written confirmation of the version and the fix for each site by the end of this week. Thank you.*

The weakness behind it

The record classes this as CWE-502.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record describes an unauthenticated flaw in a plugin on a public WordPress site, so it would likely be used to get in through the web application.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The advisory says the flaw lets an attacker make the site run harmful actions on the server, so it would typically lead to attacker-chosen commands or code running there.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *Deserialization of Untrusted Data vulnerability in Barn2 Plugins Document Library Pro document-library-pro allows Object Injection.This issue affects Document Library Pro: from n/a before 4.2.2.*

Versions of Barn2 Plugins Document Library Pro the record lists as affected:

- all versions before 4.2.2

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

What the record says to do about it, in the vendor's words:

> *Update the WordPress Document Library Pro plugin to the latest available version (at least 4.2.2).*

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-2026-122662
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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-2026-122662
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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 sources do not say whether a deactivated copy of the plugin can be attacked.
- They do not say what the attacker can do on the server beyond running harmful actions.
- They do not say whether any attack has been seen. The record is new and is not on CISA's list.
- They do not say what conditions the site needs for the flaw to be reachable.
- 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 16 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", "Likely ATT&CK mapping", "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-2026-122662: 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
15 November 2026	CVE record published by Patchstack.

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
A public website runs Document Library Pro on a version before 4.2.2	Medium	This week
The plugin is installed but switched off on a site	Medium	Next patch cycle; update or remove it
A site you cannot reach from outside runs an affected version	Medium	Next patch cycle
The plugin is on 4.2.2 or later	Low	Record the version; nothing more
You do not run WordPress or this plugin	None	None for this CVE

Appendix 4. Definition of done

- Every Barn2 Plugins Document Library Pro 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-2026-122662: https://www.cve.org/CVERecord?id=CVE-2026-122662
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: patchstack.com/database/wordpress/plugin/document-library-pro/: https://patchstack.com/database/wordpress/plugin/document-library-pro/vulnerability/wordpress-document-library-pro-plugin-4-2-2-php-object-injection-vulnerability?_s_id=cve