contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

themagnifico52 Hotel Booking Lite: new CVE

CVE-2026-125851 · record published 13 November 2026

Analysis Report

Hotel Booking Lite at version 2.5.1 or earlier has no official patch and a subscriber-level account is enough to exploit it; the Patchstack source warns this type of flaw is used in mass-exploit …

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/themagnifico52-hotel-booking-lite-cve-2026-125851

The bottom line

> *Hotel Booking Lite at version 2.5.1 or earlier has no official patch and a subscriber-level account is enough to exploit it; the Patchstack source warns this type of flaw is used in mass-exploit campaigns against thousands of sites regardless of size. Check whether the theme is installed, then disable user registration until a patch is released.*

At a glance

Fact	Detail
Product	themagnifico52 Hotel Booking Lite (CVE-2026-125851)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Patchstack on 13 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 13 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No official patch is available. The CVE record lists no unaffected version. Patchstack reported this on 11 November 2026 and states no patch exists.
Who looks first	WordPress site owners running Hotel Booking Lite at or below version 2.5.1. The Patchstack source also names 2.5.2 as vulnerable; the CVE record does not. Sites that allow visitor account registration carry the highest risk.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run the Hotel Booking Lite WordPress theme?	Nothing to do for this CVE.	Check the installed version.
Is the installed version 2.5.1 or earlier?	The CVE record does not name a later version as affected; watch for a vendor patch.	Continue — no patch exists yet; see the next question.
Can visitors register as subscribers on the site?	Risk is lower; audit existing subscriber accounts and monitor for a patch.	Disable registration until a patch is released.

What it is

An attacker who holds a subscriber-level WordPress account can upload a PHP web shell to the server. This gives them the ability to run commands and read files using the web server's own permissions.

What the vendor's advisory says

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

- The Patchstack source, published 11 November 2026, states no official patch is available and that Patchstack has issued a virtual mitigation rule to block attacks until a patch can be tested and applied. No other CVEs are mentioned alongside this one.

Things people will get wrong

- "Our site is too small to be targeted." The Patchstack source says this type of flaw is used in mass-exploit campaigns against thousands of sites regardless of traffic size or popularity.
- "Version 2.5.2 is safe." Patchstack lists 2.5.2 as vulnerable. The CVE record names 2.5.1 as the ceiling. Neither source names a fixed version. Treat 2.5.2 as affected until the vendor confirms otherwise.

How we would triage it

This is our judgement.

Step 1: Find the version you run

- In the WordPress admin panel go to Appearance → Themes and note the version shown for Hotel Booking Lite.
- Compare it against the affected range: the CVE record says through 2.5.1; the Patchstack source also names 2.5.2 as vulnerable.

Step 2: Restrict user registration

- In Settings → General, uncheck 'Anyone can register' until an official patch is available.
- Review existing subscriber accounts and remove any that are unrecognised.

Step 3: Apply Patchstack virtual mitigation if available

- If the site uses Patchstack, confirm the mitigation rule for CVE-2026-125851 is active in the Patchstack dashboard.
- If Patchstack is not in use, consider a WAF rule that blocks PHP file uploads to the theme's upload path.

Step 4: Watch for an official patch

- Monitor the Hotel Booking Lite page on WordPress.org and the Patchstack advisory for a patched version release.
- Apply the patch and re-enable registration only after confirming the fixed version is listed.

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 a vulnerability report affecting our website. CVE-2026-125851 affects the Hotel Booking Lite WordPress theme at version 2.5.1 and earlier (the Patchstack source also names 2.5.2). An attacker with a subscriber-level account can upload a malicious file and take control of the server. No official patch is available as of 11 November 2026. Please confirm whether this theme is installed, which version is running, whether user registration is currently enabled, and what interim steps are in place. We would like written confirmation of the installed version and the action taken by [DATE].*

The weakness behind it

The record classes this as CWE-434.

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 flaw is in a public-facing WordPress application; a subscriber would likely upload a malicious file over HTTP as the initial access step.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	A web shell placed on the server would typically enable command execution through a scripting interpreter running as the web server process.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	The web server process usually runs with limited privileges; a web shell would likely be used to attempt further privilege escalation on the host.

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:

> *Unrestricted Upload of File with Dangerous Type vulnerability in themagnifico52 Hotel Booking Lite hotel-booking-lite allows Upload a Web Shell to a Web Server.This issue affects Hotel Booking Lite: from n/a through 2.5.1.*

Versions of themagnifico52 Hotel Booking Lite the record lists as affected:

- all versions up to and including 2.5.1

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-2026-125851
```

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-2026-125851
```

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

- Whether the vendor has acknowledged the report or committed to a release timeline for a patch.
- Whether the upload requires the hotel booking form to be active, or only standard WordPress user registration.
- Whether uploaded files land in a web-accessible directory, which determines whether a web shell can be called remotely.
- 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 13 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", "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-2026-125851: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/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	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond 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
13 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
Hotel Booking Lite <= 2.5.1 installed, user registration open to the public	Medium	This week
Hotel Booking Lite <= 2.5.1 installed, only known staff accounts, no open registration	Medium	This week
Site on shared hosting; a web shell could affect neighbouring accounts on the same server	Medium	This week
Patchstack virtual mitigation rule active on the site	Low	Next patch cycle
Hotel Booking Lite is not installed on the site	None	None for this CVE

Appendix 4. Definition of done

- Every themagnifico52 Hotel Booking Lite 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-2026-125851: https://www.cve.org/CVERecord?id=CVE-2026-125851
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: patchstack.com/database/wordpress/theme/hotel-booking-lite/vul: https://patchstack.com/database/wordpress/theme/hotel-booking-lite/vulnerability/wordpress-hotel-booking-lite-theme-2-5-1-arbitrary-file-upload-vulnerability?_s_id=cve