



# WordPress avalex plugin <= 3.1.3 - Broken Access Control vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2026-25462                                                                                                               |
| <b>State</b>           | PUBLISHED                                                                                                                    |
| <b>Assigner</b>        | Patchstack                                                                                                                   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2026-03-25 17:16:52 UTC                                                                                                      |
| <b>Updated</b>         | 2026-04-24 16:35:20 UTC                                                                                                      |
| <b>Description</b>     | Missing Authorization vulnerability in avalex avalex avalex allows Exploiting Incorrectly Configured Access Control Security |

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

**EPSS:** 0.000540000 probability, percentile 0.168030000 (date 2026-04-26)

**Problem Types:** CWE-862 | CWE-862 Missing Authorization

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | ADP                                  | DECLARED  | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L |
| 3.1     | audit@patchstack.com                 | Secondary | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L |
| 3.1     | CNA                                  | CVSS      | 6.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

#### Vendor Declared Affected Products

| Source | Vendor                 | Product                | Version               | Platforms     |
|--------|------------------------|------------------------|-----------------------|---------------|
| CNA    | <a href="#">Avalex</a> | <a href="#">Avalex</a> | affected 3.1.3 custom | Not specified |

#### References

| Reference                                                                                       | Source                                                         | Link                           | Tags           |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------|----------------|
| <a href="#">patchstack.com/database/Wordpress/Plugin/avalex/vulnerability/wordpress-aval...</a> | <a href="mailto:audit@patchstack.com">audit@patchstack.com</a> | <a href="#">patchstack.com</a> |                |
| CVE Program record                                                                              | CVE.ORG                                                        | <a href="#">www.cve.org</a>    | canonical      |
| NVD vulnerability detail                                                                        | NVD                                                            | <a href="#">nvd.nist.gov</a>   | canonical, and |

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Nabil Irawan | Patchstack Bug Bounty Program (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)