



# WordPress Survey Maker plugin <= 3.2.0 - Broken Access Control vulnerability

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-22697   |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | Patchstack   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2024-12-13 15:15:10 UTC  |
| <b>Updated</b>         | 2026-04-23 15:17:16 UTC  |
| <b>Description</b>     | Missing Authorization vulnerability in Ays Pro Survey Maker survey-maker allows Exploiting Incorrectly Configured Access ( |

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from nvd@nist.gov

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

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

| Version | Source               | Type      | Score | Severity | Vector                                       |
|---------|----------------------|-----------|-------|----------|--|
| 3.1     | nvd@nist.gov         | Primary   | 9.8   | CRITICAL | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 3.1     | audit@patchstack.com | Secondary | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 3.1     | CNA                  | CVSS      | 5.3   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                  | Product                      | Version | Update | Edition | Language |
|-------------|-------------------------|------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Ays-pro</a> | <a href="#">Survey Maker</a> | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor                  | Product                      | Version               | Platforms     |
|--------|-------------------------|------------------------------|-----------------------|---------------|
| CNA    | <a href="#">Ays Pro</a> | <a href="#">Survey Maker</a> | affected 3.2.0 custom | Not specified |

### References

| Reference   | Source                               | Link                           | Tags          |
|---|--------------------------------------|--------------------------------|---------------|
| <a href="#">patchstack.com/database/Wordpress/Plugin/survey-maker/vulnerability/wordpres...</a> | <a href="#">audit@patchstack.com</a> | <a href="#">patchstack.com</a> | Third Party / |
| CVE Program record  | CVE.ORG                              | <a href="#">www.cve.org</a>    | canonical     |
| NVD vulnerability detail  | NVD                                  | <a href="#">nvd.nist.gov</a>   | canonical, a  |

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** [Fariq Fadillah Gusti Insani | 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](#)