



# WordPress Survey Maker plugin <= 5.1.6.3 - Bypass vulnerability

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

## Summary

<b>CVE</b>	CVE-2025-32275
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-04-10 08:15:20 UTC
<b>Updated</b>	2026-04-01 17:22:18 UTC
<b>Description</b>	Authentication Bypass by Spoofing vulnerability in Ays Pro Survey Maker survey-maker allows Identity Spoofing.This issue

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-290 | CWE-290 Authentication Bypass by Spoofing

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

### 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 5.1.6.3 custom	Not specified

### References

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

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** [Martino Spagnuolo \(r3verii\)](#) | [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)