



# Quiz And Survey Master <= 10.3.1 - Missing Authorization to Authenticated (Subscriber+) Quiz Results Deletion

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

## Summary

<b>CVE</b>	CVE-2025-9294
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-01-06 09:15:55 UTC
<b>Updated</b>	2026-04-08 18:25:26 UTC
<b>Description</b>	The Quiz and Survey Master (QSM) – Easy Quiz and Survey Maker plugin for WordPress is vulnerable to unauthorized los

## Risk And Classification

**Primary CVSS:** v3.1 4.3 MEDIUM from security@wordfence.com

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

**EPSS:** 0.000390000 probability, percentile 0.118810000 (date 2026-04-08)

**Problem Types:** CWE-285 | CWE-862 | CWE-285 CWE-285 Improper Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/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	Expresstech	Quiz And Survey Master	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Expresstech	Quiz And Survey Master QSM Easy Quiz And Survey Maker	affected 10.3.1 semver	Not specified

### References

Reference	Source	Link
<a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/55895508-d0ef-4855-8d15-b8a45...">www.wordfence.com/threat-intel/vulnerabilities/id/55895508-d0ef-4855-8d15-b8a45...</a>	security@wordfence.com	<a href="http://www.wordfence.com">www.wordfence.com</a>
<a href="http://research.cleantalk.org/cve-2025-9294">research.cleantalk.org/cve-2025-9294</a>	security@wordfence.com	<a href="http://research.cleantalk.org">research.cleantalk.org</a>
<a href="http://plugins.trac.wordpress.org/browser/quiz-master-next/tags/10.2.6/php/admin/options-page-q...">plugins.trac.wordpress.org/browser/quiz-master-next/tags/10.2.6/php/admin/options-page-q...</a>	security@wordfence.com	<a href="http://plugins.trac.wordpress.org">plugins.trac.wordpress.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Dmitrii Ignatyev (en)

### Additional Advisory Data

Source	Time	Event
CNA	2025-08-13T00:00:00.000Z	Discovered
CNA	2026-01-05T20:13:08.000Z	Disclosed

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

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](https://cve.report/api)

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