



# RSVPMaker <= 9.3.2 - Unauthenticated SQL Injection

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

## Summary

<b>CVE</b>	CVE-2022-1768
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-06-13 14:15:08 UTC
<b>Updated</b>	2026-04-08 19:17:49 UTC
<b>Description</b>	The RSVPMaker plugin for WordPress is vulnerable to unauthenticated SQL Injection due to insufficient escaping and para

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

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

**EPSS:** 0.861120000 probability, percentile 0.993950000 (date 2026-04-08)

**Problem Types:** CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/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

None

Availability

None

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Carrcommunications</a>	<a href="#">Rsvpmaker</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Davidfcarr</a>	<a href="#">RSVPMaker</a>	affected 9.3.2 semver	Not specified

### References

Reference	Source
WordPress RSVPMaker 9.3.2 SQL Injection ~ Packet Storm	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>
Vulnerability Advisories - Wordfence	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>
403 Forbidden	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>
WordPress Plugin RSVPMaker <= 9.3.2 - Unauthenticated SQL Injection vulnerability · GitHub	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>
RSVPMaker <= 9.3.2 - Unauthenticated SQL Injection	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>
CVE Program record	CVE.ORG

## Vendor Comments And Credit

## Discovery Credit

**CNA:** Muhammad Zeeshan (en)

## Additional Advisory Data

Source	Time	Event
CNA	2022-05-17T00:00:00.000Z	Disclosed

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](#)