



# WP SMS <= 6.5 - Authenticated (Admin+) SQL Injection to Reflected Cross-Site Scripting

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

## Summary

<b>CVE</b>	CVE-2023-6981
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-01-03 06:15:47 UTC
<b>Updated</b>	2026-04-08 19:19:03 UTC
<b>Description</b>	The WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc plugin for WordPress is v

## Risk And Classification

**Primary CVSS:** v3.1 4.9 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.003460000 probability, percentile 0.572720000 (date 2026-04-16)

**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	4.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
3.1	security@wordfence.com	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Veronalabs	Wp Sms	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	F
CNA	Veronalabs	WSMS Formerly WP SMS SMS MMS Notifications With OTP And 2FA For WooCommerce	affected 6.5 semver	N

#### References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/b8f53053-5150-4fba-b8d6-3d6c9...	af854a3a-2127-422b-91ae-364da2661108	www.wc
github.com/wp-sms/wp-sms/commit/6656de201efe67c7983102c344a546eed976a819	af854a3a-2127-422b-91ae-364da2661108	github.c
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Krzysztof Zajac (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2024-01-02T00:00:00.000Z	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)