



WP SMS <= 6.5 - Cross-Site Request Forgery to Subscriber Deletion

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

Summary

CVE	CVE-2023-6980
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-03 06:15:47 UTC
Updated	2026-04-08 18:18:46 UTC
Description	The WP SMS – Messaging & SMS Notification for WordPress, WooCommerce, GravityForms, etc plugin for WordPress is v

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/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	Product
CNA	Veronalabs	WSMS Formerly WP SMS SMS MMS Notifications With OTP And 2FA For WooCommerce	affected 6.5 semver	N

References

Reference	Source	Link
github.com/wp-sms/wp-sms/commit/0f36e2f521ade8ddfb3e04786defe074370afb50	af854a3a-2127-422b-91ae-364da2661108	github.co
www.wordfence.com/threat-intel/vulnerabilities/id/94ad6b51-ff8d-48d5-9a70-1781d...	af854a3a-2127-422b-91ae-364da2661108	www.wor
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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.

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