

WordPress WM Options Import Export plugin <= 1.0.1 - Sensitive Data Exposure vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF 

Summary	
CVE	CVE-2025-23781
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-22 15:15:23 UTC
Updated	2026-04-23 15:24:30 UTC
Description	Insertion of Sensitive Information Into Sent Data vulnerability in Web Mumbai WM Options Import Export wm-options-import-export

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from audit@patchstack.com

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

Problem Types: CWE-201 | CWE-201 Insertion of Sensitive Information Into Sent Data

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Web Mumbai	WM Options Import Export	affected 1.0.1 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/wm-options-import-export/vulnerabil...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar



Vendor Comments And Credit

Discovery Credit

CNA: Mika | Patchstack Bug Bounty Program (en)

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