



YML for Yandex Market < 5.0.26 - Shop Manager+ RCE via Feed Generation

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

Summary

CVE	CVE-2025-14545
State	PUBLISHED
Assigner	WPScan
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 07:16:19 UTC
Updated	2026-04-13 15:02:06 UTC
Description	The YML for Yandex Market WordPress plugin before 5.0.26 is vulnerable to Remote Code Execution via the feed generati

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.000790000 probability, percentile 0.234020000 (date 2026-04-14)

Problem Types: CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Unknown	YML For Yandex Market	affected 5.0.26 semver	Not specified

References

Reference	Source	Link	Tags
wpscan.com/vulnerability/9bb1a4ca-976c-461d-82de-8a3b04a56fbc	contact@wpscan.com	wpscan.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Alex Tselevich (nos3curity) (en)

CNA: WPScan (en)

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