



# VK Blocks <= 1.57.0.5 - Authenticated(Contributor+) Settings Update

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

## Summary

<b>CVE</b>	CVE-2023-0584
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-03 02:15:09 UTC
<b>Updated</b>	2026-04-08 19:18:01 UTC
<b>Description</b>	The VK Blocks plugin for WordPress is vulnerable to improper authorization via the REST 'update_options' function in versi

## Risk And Classification

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

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

**EPSS:** 0.000630000 probability, percentile 0.195550000 (date 2026-04-09)

**Problem Types:** CWE-285 | NVD-CWE-Other | CWE-285 CWE-285 Improper Authorization

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

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vektor-inc	Vk Blocks	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vektor-inc	VK Blocks	affected 1.57.0.5 semver	Not specified

### References

Reference	Source	Link
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	<a href="https://plugins.trac.wordpress.org/">plugins.trac.wordpress.o</a>
<a href="https://plugins.trac.wordpress.org/changeset/2927751">plugins.trac.wordpress.org/changeset/2927751</a>	security@wordfence.com	<a href="https://plugins.trac.wordpress.org/">plugins.trac.wordpress.o</a>
VK Blocks <= 1.57.0.5 - Authenticated(Contributor+) Settings Update	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.wordfence.com">www.wordfence.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Ramuel Gall (en)

### Additional Advisory Data

Source	Time	Event
CNA	2023-01-30T00:00:00.000Z	Discovered
CNA	2023-06-02T00:00:00.000Z	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)