



# Spectra Pro <= 1.1.5 - Authenticated (Author+) Privilege Escalation

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

## Summary

<b>CVE</b>	CVE-2024-3828
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-05-14 15:42:24 UTC
<b>Updated</b>	2026-04-08 19:21:28 UTC
<b>Description</b>	The Spectra Pro plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.1.5. This is

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from security@wordfence.com

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

**EPSS:** 0.001390000 probability, percentile 0.339880000 (date 2026-04-12)

**Problem Types:** CWE-269 | CWE-269 CWE-269 Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Brainstorm Force</a>	<a href="#">Spectra Pro</a>	affected 1.1.5 semver	Not specified
ADP	<a href="#">Brainstormforce</a>	<a href="#">Spectra Pro</a>	affected 1.1.5	Not specified

### References

Reference	Source	Link
<a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/e23e7d66-4b57-4feb-bf77-46238...">www.wordfence.com/threat-intel/vulnerabilities/id/e23e7d66-4b57-4feb-bf77-46238...</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.wordfence.com">www.wor</a>
<a href="http://wpspectra.com/whats-new">wpspectra.com/whats-new</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://wpspectra.com">wpspectr</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.g</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Ngô Thiên An (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-05-09T18:13:16.000Z	Disclosed

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)