



# WordPress RewardsWP plugin <= 1.0.4 - Privilege Escalation vulnerability

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

## Summary

<b>CVE</b>	CVE-2026-32520
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 17:17:04 UTC
<b>Updated</b>	2026-03-30 13:27:12 UTC
<b>Description</b>	Incorrect Privilege Assignment vulnerability in Andrew Munro / AffiliateWP RewardsWP rewardswp allows Privilege Escalat

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from ADP

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

**EPSS:** 0.000540000 probability, percentile 0.172720000 (date 2026-04-05)

**Problem Types:** CWE-266 | CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Andrew Munro AffiliateWP</a>	<a href="#">RewardsWP</a>	affected n/a <= 1.0.4 custom	Not specified

### References

Reference	Source	Link	Tags
<a href="https://patchstack.com/database/Wordpress/Plugin/rewardswp/vulnerability/wordpress-r...">patchstack.com/database/Wordpress/Plugin/rewardswp/vulnerability/wordpress-r...</a>	<a href="mailto:audit@patchstack.com">audit@patchstack.com</a>	<a href="https://patchstack.com">patchstack.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ar

### Vendor Comments And Credit

Discovery Credit  
**CNA: daroo | Patchstack Bug Bounty Program (en)**

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