



# WordPress Cryptocurrency Widgets – Price Ticker & Coins List Plugin <= 2.6.8 is vulnerable to Broken Access Control

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

## Summary

<b>CVE</b>	CVE-2024-27953
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-13 17:15:48 UTC
<b>Updated</b>	2026-04-28 19:23:34 UTC
<b>Description</b>	Missing Authorization vulnerability in Cool Plugins Cryptocurrency Widgets – Price Ticker & Coins List.This issue affects Cr

## Risk And Classification

**Primary CVSS:** v3.1 4.7 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.001070000 probability, percentile 0.286060000 (date 2026-04-28)

**Problem Types:** CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
3.1	audit@patchstack.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Coolplugins	Cryptocurrency Widgets	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cool Plugins	Cryptocurrency Widgets Price Ticker Coins List	affected n/a 2.6.8 custom	Not specified

### References

Reference	Source	Link
patchstack.com/database/vulnerability/cryptocurrency-price-ticker-widget/wor...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

### Vendor Comments And Credit

Discovery Credit

**CNA:** CatFather (Patchstack Alliance) (en)

### Additional Advisory Data

Solutions

**CNA:** Update to 2.6.9 or a higher version.

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

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)