



# WordPress Apollo13 Framework Extensions plugin <= 1.8.10 - Broken Access Control

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

## Summary

<b>CVE</b>	CVE-2023-25959
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-12-09 13:15:24 UTC
<b>Updated</b>	2026-04-28 19:19:52 UTC
<b>Description</b>	Missing Authorization vulnerability in Apollo13Themes Apollo13 Framework Extensions allows Exploiting Incorrectly Config

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from audit@patchstack.com

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

**EPSS:** 0.001170000 probability, percentile 0.300980000 (date 2026-05-01)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Apollo13Themes</a>	<a href="#">Apollo13 Framework Extensions</a>	affected n/a 1.8.10 custom	Not specified

### References

#### Reference

[patchstack.com/database/wordpress/plugin/apollo13-framework-extensions/vulne...](https://patchstack.com/database/wordpress/plugin/apollo13-framework-extensions/vulnerability/wordpress-apollo13-framework-extensions-plu)

<https://patchstack.com/database/wordpress/plugin/apollo13-framework-extensions/vulnerability/wordpress-apollo13-framework-extensions-plu>

[CVE Program record](#)

[NVD vulnerability detail](#)

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** István Márton (Patchstack Alliance) (en)

### Additional Advisory Data

#### Solutions

**CNA:** No patched version is available. We notified the vendor about the vulnerability on 2023 Jan 12th.

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](#)