



Broken Access Control vulnerability affecting multiple WordPress themes by Extend Themes

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

Summary

CVE	CVE-2024-33686
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-29 06:15:16 UTC
Updated	2026-04-28 19:25:12 UTC
Description	Missing Authorization vulnerability in Extend Themes Pathway, Extend Themes Hugo WP, Extend Themes Althea WP, Ext

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.002480000 probability, percentile 0.480520000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.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	CVSS	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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Extend Themes	Pathway	affected n/a 1.0.15 custom	Not specified
CNA	Extend Themes	Hugo WP	affected n/a 1.0.8 custom	Not specified
CNA	Extend Themes	Althea WP	affected n/a 1.0.13 custom	Not specified
CNA	Extend Themes	Elevate WP	affected n/a 1.0.15 custom	Not specified
CNA	Extend Themes	Brite	affected n/a 1.0.11 custom	Not specified
CNA	Extend Themes	Colibri WP	affected n/a 1.0.94 custom	Not specified
CNA	Extend Themes	Vertice	affected n/a 1.0.7 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/vertice/wordpress-vertice-theme-1-0-7-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/vulnerability/elevate-wp/wordpress-elevate-wp-theme-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/vulnerability/colibri-wp/wordpress-colibri-wp-theme-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/vulnerability/brite/wordpress-brite-theme-1-0-11-bro...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/vulnerability/hugo-wp/wordpress-hugo-wp-theme-1-0-8-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/vulnerability/althea-wp/wordpress-althea-wp-theme-1-...	af854a3a-2127-422b-91ae-364da2661108	patchstack.com
patchstack.com/database/vulnerability/pathway/wordpress-pathway-theme-1-0-15-...	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: Dhabaleshwar Das (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update Pathway to 1.0.16, Hugo WP to 1.0.10, Althea WP to 1.0.16, Elevate WP to 1.0.17, Brite to 1.0.15, Colibri WP to 1.0.99, Vertice to 1.0.11 or higher versions.

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](#)