WordPress Checkout Mestres WP plugin <= 8.6 - Local File Inclusion vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-44030
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-02 10:15:04 UTC
Updated	2026-04-23 15:19:02 UTC
Description	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mestres do WP Checkout Mes

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from audit@patchstack.com

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

Problem Types: CWE-22 | CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
High

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mestres Do WP	Checkout Mestres WP	affected 8.6 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/checkout-mestres-wp/vulnerability/w...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: tahu.datar | Patchstack Bug Bounty Program (en)

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