



WordPress WP Time Slots Booking Form plugin <= 1.1.82 - Broken Access Control vulnerability

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

Summary

CVE	CVE-2023-23895
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-09 13:15:21 UTC
Updated	2026-04-28 19:19:34 UTC
Description	Missing Authorization vulnerability in CodePeople WP Time Slots Booking Form allows Exploiting Incorrectly Configured Ac

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
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

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Codepeople	Wp Time Slots Booking Form	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CodePeople	WP Time Slots Booking Form	affected n/a 1.1.82 custom	Not specified

References

Reference

patchstack.com/database/wordpress/plugin/wp-time-slots-booking-form/vulnerab...

<https://patchstack.com/database/wordpress/plugin/wp-time-slots-booking-form/vulnerability/wordpress-wp-time-slots-booking-form-plugin-1-1-82>

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: yuyudhn (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress WP Time Slots Booking Form plugin to the latest available version (at least 1.1.83).

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

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