



WordPress DirectoryPress plugin <= 3.6.2 - Unauthenticated Broken Access Control Vulnerability

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

Summary

CVE	CVE-2023-37967
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-13 15:15:18 UTC
Updated	2026-04-28 19:20:57 UTC
Description	Missing Authorization vulnerability in Designinvento DirectoryPress allows Exploiting Incorrectly Configured Access Control

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.002470000 probability, percentile 0.479770000 (date 2026-05-13)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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	Designinvento	Directorypress	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Designinvento	DirectoryPress	affected n/a 3.6.2 custom	Not specified

References

Reference

patchstack.com/database/wordpress/plugin/directorypress/vulnerability/wordpr...

<https://patchstack.com/database/wordpress/plugin/directorypress/vulnerability/wordpress-directorypress-plugin-3-6-2-unauthenticated-broken->

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: [Abdi Pranata \(Patchstack Alliance\)](#) (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress DirectoryPress plugin to the latest available version (at least 3.6.3).

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

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