



WordPress leyka plugin <=3.31.6 - Broken Access Control vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2024-49252
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-16 14:15:10 UTC
Updated	2026-04-23 15:19:31 UTC
Description	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in VaultDweller Leyka leyka. This

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from audit@patchstack.com

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

Problem Types: CWE-497 | CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	VaultDweller	Leyka	affected 3.31.6 custom	Not specified
ADP	Teplitsa Of Social Technologies	Leyka	affected 3.31.6 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/leyka/vulnerability/wordpress-leyka...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

Vendor Comments And Credit

Discovery Credit

CNA: Trương Hữu Phúc (truonghuuphuc) | Patchstack Bug Bounty Program (en)

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