WordPress One Click Demo Import plugin <=3.2.0 - PHP Object Injection vulnerability

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

Summary

CVE	CVE-2024-34433
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-14 15:39:03 UTC
Updated	2026-04-28 19:25:24 UTC
Description	Deserialization of Untrusted Data vulnerability in OCDI One Click Demo Import.This issue affects One Click Demo Import: f

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

EPSS: 0.004170000 probability, percentile 0.617640000 (date 2026-04-28)

Problem Types: CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

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	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

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	Ocdi	One Click Demo Import	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OCDI	One Click Demo Import	affected n/a 3.2.0 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/one-click-demo-import/wordpress-one-cl...	af854a3a-2127-422b-91ae-364da2661108	patchstack.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: ngductung (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 3.2.1 or a higher version.

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

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