WordPress Catalyst Connect Zoho CRM Client Portal Plugin <= 2.0.0 is vulnerable to Cross Site Scripting (XSS)

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

Summary

CVE	CVE-2022-44629
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-10 10:15:09 UTC
Updated	2026-04-28 19:18:55 UTC
Description	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Catalyst Connect Catalyst Connect Zoho CRM Client Port

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Catalystconnect	Catalyst Connect Zoho Crm Client Portal	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Catalyst Connect	Catalyst Connect Zoho CRM Client Portal	affected n/a 2.0.0 custom	Not specified

References

Reference	Sc
WordPress Catalyst Connect Zoho CRM Client Portal plugin <= 2.0.0 - Auth. Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	af
CVE Program record	CV
NVD vulnerability detail	NV

Vendor Comments And Credit

Discovery Credit

CNA: Hoang Van Hiep aka sk4rl1ghT (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.1.0 or a higher version.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**