WordPress Progress Planner plugin <= 0.9.2 - Cross Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2024-37422
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-07-22 09:15:09 UTC
Updated	2026-04-01 16:17:25 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Progress Planner Prog

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

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

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

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
Required

Scope
Changed

Confidentiality
Low

Integrity
Low

Availability
None

CVSS:3.1/AV:N/AC:L/PR:L/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	Emilia	Progress Planner	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Progress Planner	Progress Planner	affected 0.9.2 custom	Not specified
ADP	Emilia	Progress Planner	affected 0.9.2 semver	Not specified

References

Reference	Source	Link
patchstack.com/database/Wordpress/Plugin/progress-planner/vulnerability/word...	audit@patchstack.com	patchstack.c
patchstack.com/database/vulnerability/progress-planner/wordpress-progress-pl...	af854a3a-2127-422b-91ae-364da2661108	patchstack.c
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: justakazh | Patchstack Bug Bounty Program (en)

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