WordPress PixTypes plugin <= 1.4.15 - Cross Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2023-40205
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-04 12:15:09 UTC
Updated	2026-04-23 15:17:37 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in pixelgrade PixTypes pi

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/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')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/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	Pixelgrade	Pixtypes	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pixelgrade	PixTypes	affected 1.4.15 custom	Not specified

References

Reference	Source	Li
WordPress PixTypes plugin <= 1.4.15 - Cross Site Scripting (XSS) vulnerability - Patchstack	af854a3a-2127-422b-91ae-364da2661108	pa
patchstack.com/database/Wordpress/Plugin/pixtypes/vulnerability/wordpress-pi...	audit@patchstack.com	pa
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

CNA: minhtuanact | Patchstack Bug Bounty Program (en)

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