



WordPress SAHU TikTok Pixel for E-Commerce Plugin <= 1.2.2 is vulnerable to Cross Site Scripting (XSS)

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-46642
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-08 17:15:07 UTC
Updated	2026-04-28 19:21:45 UTC
Description	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in sahumedia SAHU TikTok Pixel for E-Commerce plugin <=

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

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	Sahu	Sahu Tiktok Pixel For E-commerce	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sahumedia	SAHU TikTok Pixel For E-Commerce	affected n/a 1.2.2 custom	Not specified

References

Reference	Source
WordPress SAHU TikTok Pixel for E-Commerce plugin <= 1.2.2 - Cross Site Scripting (XSS) vulnerability - Patchstack	af854a3a-2127-422b
patchstack.com/database/Wordpress/Plugin/sahu-tiktok-pixel/vulnerability/wor...	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Rio Darmawan (Patchstack Alliance) (en)

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