WordPress Gyan Elements plugin <= 2.2.1 - Reflected Cross Site Scripting (XSS) vulnerability

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

Summary

CVE	CVE-2026-23979
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 17:16:36 UTC
Updated	2026-04-24 16:32:53 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Softwebmedia Gyan El

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from ADP

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

EPSS: 0.000390000 probability, percentile 0.118180000 (date 2026-04-26)

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	ADP	DECLARED	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
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	134c704f-9b21-4f2e-91b3-4a467353bcc0	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

Integrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Softwebmedia	Gyan Elements	affected 2.2.1 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/gyan-elements/vulnerability/wordpre...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: João Pedro S Alcântara (Kinorth) | Patchstack Bug Bounty Program (en)

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