



WordPress bunny.net plugin <= 2.3.0 - Cross Site Scripting (XSS) Vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2025-48236
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-19 15:15:26 UTC
Updated	2026-04-23 15:30:56 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bunny.net bunny.net b

Risk And Classification

Primary CVSS: v3.1 8.5 HIGH from audit@patchstack.com

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

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	audit@patchstack.com	Secondary	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L
3.1	CNA	CVSS	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Bunny.net	Bunny.net	affected 2.3.0 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/bunnycdn/vulnerability/wordpress-bu...	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: Peter Thaleikis | Patchstack Bug Bounty Program (en)

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