



WordPress Entrada theme <= 5.7.7 - Cross Site Request Forgery (CSRF) vulnerability

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2025-58918
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-27 03:15:50 UTC
Updated	2026-04-28 19:34:22 UTC

Description Cross-Site Request Forgery (CSRF) vulnerability in Waituk Entrada theme allows Cross Site Request Forgery.This issue af

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.000150000 probability, percentile 0.029660000 (date 2026-04-28)

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Waituk	Entrada	affected n/a 5.7.7 custom	Not specified

References

Reference

patchstack.com/database/WordPress/Theme/entrada/vulnerability/wordpress-entr...

https://patchstack.com/database/WordPress/Theme/entrada/vulnerability/wordpress-entrada-theme-5-7-7-cross-site-request-forgery-csrf-vulne

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Tran Nguyen Bao Khanh (VCI - VNPT Cyber Immunity) | Patchstack Bug Bounty Program (en)

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