



WordPress Essential Breadcrumbs plugin <= 1.1.1 - CSRF to Privilege Escalation vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-31038
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-09 17:15:35 UTC
Updated	2026-04-23 15:27:35 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in Essential Marketer Essential Breadcrumbs essential-breadcrumbs allow

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from audit@patchstack.com

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

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Essential Marketer	Essential Breadcrumbs	affected 1.1.1 custom	Not specified

References

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



Vendor Comments And Credit

Discovery Credit

CNA: LVT-tholv2k | Patchstack Bug Bounty Program (en)

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