EasyCommerce – AI-Powered, Blazing-Fast & Beautiful WordPress Ecommerce Plugin 0.9.0-beta2 - 1.8.2 - Unauthenticated Privilege Escalation

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

Summary

CVE	CVE-2025-11457
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-11-11 04:15:41 UTC
Updated	2026-04-08 18:23:16 UTC
Description	The EasyCommerce – AI-Powered, Fast & Beautiful WordPress Ecommerce Plugin plugin for WordPress is vulnerable to P

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

EPSS: 0.001870000 probability, percentile 0.405420000 (date 2026-04-08)

Problem Types: CWE-269 | CWE-269 CWE-269 Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product
CNA	Easycommerce	EasyCommerce AI-Powered WordPress Ecommerce Plugin To Sell Digital Products Subscriptions Physical Good

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/7ebe84ba-abc1-410c-b315-11874...	security@wordfence.com	www.wordfence.c
plugins.trac.wordpress.org/changeset/3392029/easycommerce/trunk/app/Abstracts/User.php	security@wordfence.com	plugins.trac.wordp
wordpress.org/plugins/easycommerce	security@wordfence.com	wordpress.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Kenneth Dunn (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-11-10T15:10:06.000Z	Disclosed

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

CVE.report and Source URL Uptime Status status.cve.report