Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Attackers Exploit an Access Bypass in Drupal Commerce Core

Date of Publication	Admiralty Code	TA Number
November 04, 2026	A1	TA2026322

Summary

First Seen: October 28, 2026
Affected Products: Drupal Commerce Core
Impact: Drupal has disclosed an access bypass in Commerce Core, the module that powers shopping carts, checkout forms, and commerce APIs on Drupal-based online stores. Tracked as CVE-2026-118539, the flaw stems from missing authorization checks: the module does not sufficiently protect certain routes and entity fields, which allows an unauthenticated visitor to reach data and functionality that should be off-limits. Because exploitation is already confirmed, patching is the only reliable response: Drupal shipped fixed builds on October 28, 2026, with sites on the 3.x branch required to move to Commerce Core 3.3.13 and sites on earlier branches to Commerce Core 8.x-2.41. Upgrading closes the exposure but does not undo anything that happened before it, so the project also urged affected merchants to audit their orders for inconsistencies as part of the same remediation effort.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-118539	Drupal Commerce Core Access Bypass Vulnerability	Drupal Commerce Core	✓	✗	✓

Vulnerability Details

#1

CVE-2026-118539 is a missing authorization weakness, classified as CWE-862, in Drupal's Commerce Core module. Commerce Core is the contributed module that lets a Drupal site sell goods and services, either through a built-in cart and checkout flow or through decoupled front-ends that talk to the site over APIs. The module does not sufficiently protect certain routes and entity fields. In plain terms, parts of the commerce layer check who you are in some places but forget to check in others, and those unguarded paths are reachable from the open internet.

#2

The root cause is an authorization gap rather than a memory-safety or injection bug, so exploitation does not need crafted payloads or custom tooling. The CVE record describes the issue as a missing authorization vulnerability that allows forceful browsing, meaning an attacker simply requests the unprotected URLs and entity fields directly instead of navigating the site the way a normal shopper would. Drupal's own risk vector reinforces how low the bar is: access complexity is rated as none, meaning a user only has to visit a page, and authentication is rated as none, meaning anonymous visitors can do it. Confidentiality impact is listed as certain non-public data being released and integrity impact as some data being modifiable, which together explain why the project framed the consequence as something that may financially impact the vendor.

#3

The flaw affects every Commerce Core release before 2.41 as well as the 3.x branch from 3.0.0 up to but not including 3.3.13. Drupal rates target distribution as all, so no particular setting, theme, or integration is required for a site to be exploitable; if the module is installed and the version is in range, the site is in scope. The project scored the overall risk at 21 out of 25 and labelled it highly critical, its most severe classification. No CVSS base score had been assigned at the time the public reporting was published, so the Drupal risk score remains the most reliable severity signal available from the sources reviewed for this advisory.

#4

The vulnerability is being actively exploited in the wild and included that exploit status in its risk vector, which recognises that documented or deployed exploit code is already circulating, making this effectively a zero-day at the point of disclosure. The strongest operational signal given to defenders was the instruction to audit orders for inconsistencies, which suggests that observed abuse touches order data rather than being limited to passive information disclosure.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-118539	Drupal Commerce Core versions: from 0.0.0 to 2.41, from 3.0.0 to 3.3.13.	cpe:2.3:a:drupal:commerce_core:*:*:*:*:*:*:*:*	CWE-862

Recommendations

Upgrade Commerce Core Immediately: Install the fixed release without waiting for a maintenance window. Move sites on the 3.x branch to Commerce Core 3.3.13, and sites on an earlier branch to Commerce Core 8.x-2.41. Because exploitation requires no account and no unusual configuration, the time between disclosure and patching is the full exposure window for an internet-facing store.

Audit Your Orders for Inconsistencies: Drupal specifically asked site owners to do this, which is unusual and should be treated as a strong hint that order data is being touched in real attacks. Review recent orders for mismatched totals, unexpected discounts or price changes, status transitions that nobody on your team made, and shipments or refunds that do not line up with payment records. Work backwards far enough to cover the period before you patched, not just the last few days.

Review Access Logs for Forceful Browsing: Look through web server and application logs for direct requests to commerce routes and entity endpoints that bypass the normal cart and checkout journey, especially from anonymous sessions. Repeated requests to order, cart or product entity paths with no preceding browsing activity are the behavioural pattern to hunt for, since no file hashes or network indicators have been published for this campaign.

Restrict Exposure of Commerce Endpoints: Where a patch cannot be applied right away, put compensating controls in front of the application. Rate-limit and monitor anonymous requests to commerce routes at the web application firewall or reverse proxy, and tighten access to any decoupled API surface so that only expected clients can reach it. Treat these as a stopgap that buys time, not as a substitute for upgrading.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Collection	T1213: Data from Information Repositories	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://www.drupal.org/sa-contrib-2026-254

References

https://www.drupal.org/sa-contrib-2026-254

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 04, 2026 • 05:40 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com