

# WooCommerce WordPress Plugin Exploit Enables Fraudulent Charges via @sejournal, @martinibuster

The popular WooCommerce Square plugin for WordPress vulnerability enables unauthenticated attackers to uncover credit cards on file and make fraudulent charges. The vulnerability affects up to 80,000 installations.

## WooCommerce Square WordPress Plugin

The WooCommerce Square plugin enables WordPress sites to accept payments through the Square POS, as well as synchronize product inventory data between Square and WooCommerce. Square plugin enables a WooCommerce merchant to support payments through Apple Pay®, Google Pay, WooCommerce Pre-Orders, and WooCommerce Subscriptions.

## Insecure Direct Object Reference

The vulnerability in the plugin arises from an Insecure Direct Object Reference (IDOR) vulnerability, a flaw that happens when critical data is exposed in URL file parameters, such as identification numbers, which then enables an attacker to manipulate that data without proper access that would normally prevent them from accessing those files.

The Open Worldwide Application Security Project (OWASP) defines IDOR as:

*“Insecure Direct Object Reference (IDOR) is a vulnerability that arises when attackers can access or modify objects by manipulating identifiers used in a web application’s URLs or parameters. It occurs due to missing access control checks, which fail to verify whether a user should be allowed to access specific data.”*

Exploiting the vulnerability does not require that the attacker acquire any level of authentication or permission levels, making it easier for them to launch an attack on affected websites.

*According to a Wordfence advisory:*

*“The WooCommerce Square plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.1.1 via the get\_token\_by\_id function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to expose arbitrary Square “ccof” (credit card on file) values and leverage this value to potentially make fraudulent charges on the target site.”*

There are multiple versions of the WooCommerce Square plugin that are patched, it’s recommended that users of the plugin update to at least one of the following versions:

- 4.2.3
- 4.3.2
- 4.4.2
- 4.5.2
- 4.6.4
- 4.7.4
- 4.8.8
- 4.9.9
- 5.0.1
- 5.1.2

The CVSS severity vulnerability score is rated at 7.5, indicating it's a dangerous vulnerability that can be remotely exploitable but is mitigated by a constraint that keeps it from being rated as "Critical."

*Featured Image by Shutterstock/IgorZh*

<https://www.searchenginejournal.com/woocommerce-wordpress-plugin-exploit-enables-fraudulent-charges/564872/>