WPScan

WordPress Plugin Vulnerabilities

Booster for WooCommerce - Checkout Files Deletion via CSRF

Description

The plugins do not have CSRF check in place when deleting files uploaded at the checkout, allowing attackers to make a logged in shop manager or admin delete them via a CSRF attack

Proof of Concept

```
Requirements:
- Enable the "Checkout File Upload" module of the plugin (/wp-admin/admin.php?
page=wc-settings&tab=jetpack&wcj-cat=dashboard&section=all_module)

To delete the checkout files from the Order ID 1, Make a logged in shop manager or
admin open: https://example.com/wp-admin/?
wcj_download_checkout_file_admin_delete_all=1
```

Affects Plugins

 woocommerce-jetpack

Fixed in version 5.6.7 ✓

booster-plus-for-woocommerce

Fixed in version 5.6.5 ✓

booster-elite-for-woocommerce

booster-elite-for-woocommerce

WPScan

Fixed in version 1.1.7 ✓

References

CVE

CVE-2022-3763

Classification

Type

CSRF

OWASP top 10

A2: Broken Authentication and Session Management

CWE

CWE-352

Miscellaneous

Original Researcher

WPScan

Verified

Yes

WPVDB ID

7ab15530-8321-487d-97a5-1469b51fcc3f

Timeline

Publicly Published

2022-10-31 (about 25 days ago)

WPScan

Added
2022-10-31 (about 25 days ago)

Last Updated
2022-11-02 (about 23 days ago)

Our Other Services

WPScan WordPress Security Plugin

For Developers

Other
