[WordPress Plugin Vulnerabilities](#)

Easy Digital Downloads < 3.1.0.2 - Unauthenticated CSV Injection

Description

The plugin does not validate data when its output in a CSV file, which could lead to CSV injection.

Proof of Concept

```
- Submit an order using =5+5 as "first name" and empty "last name" (the plugin allows
  that).
- Export the data as CSV from Reports > Export.
- Open the CSV with a spreadsheet application (Excel, Libre Office).
- The CSV formula gets executed.
```

Affects Plugins

 [easy-digital-downloads](#)

Fixed in version 3.1.0.2 ✓

References

CVE
[CVE-2022-3600](#)

WPScan

Classification

Type
CSV INJECTION

OWASP top 10
A1: Injection

CWE
CWE-1236

Miscellaneous

Original Researcher
Francesco Carlucci

Submitter
Francesco Carlucci

Submitter website
https://carluc.ci

Submitter twitter
francecarlucci

Verified
Yes

WPVDB ID
16e2d970-19d0-42d1-8fb1-e7cb14ace1d0

Timeline

WPScan

Policy Published

2022-09-28 (about 1 months ago)

Added

2022-10-28 (about 28 days ago)

Last Updated

2022-10-28 (about 28 days ago)

Our Other Services

WPScan WordPress Security Plugin

Vulnerabilities

WordPress

Plugins

Themes

Our Stats

Submit vulnerabilities

About

How it works

Pricing

WPScan

WordPress plugin

News

Contact

For Developers

Status

API details

CLI scanner

Other

Privacy

Terms of service

Submission terms

Disclosure policy

In partnership with Jetpack

An   endeavor

Work With Us