$\leftrightarrow$  Code  $\odot$  Issues 178  $\,$   $\$   $\$  Pull requests  $\ \odot$  Actions  $\ \boxplus$  Projects  $\ \square$  Wiki

Jump to bottom

# Connections 0.7.3.2 <= 9.6 CSV Injection #474



rudSarkar commented on May 29, 2020

## Description

New issue

CSV Injection, also known as Formula Injection, occurs when websites embed untrusted input inside CSV files. Which lead to hijacking user's computer by exploiting with untrusted input. In this plugin, all the input fields of connections\_add are affected.

### Affected Item

Export All feature

#### Affected Version

0.7.3.2 <= 9.6

#### **Tested With**

Wordpress 5.4.1

#### Step to reproduce

- 1. Login to your website
- 2. Visit http://localhost/wordpress/wp-admin/admin.php?page=connections\_add
- 3. In the input filed add payload  $\,\, @SUM(1+1)*cmd\,|\,\,'\,\,/C\,\,\,calc'\,!\,A0$
- 4. Visit Connections Tools and then click on  $\,$  Export All
- 6. It will open CMD

#### **Exported CSV File**

Entry ID	Order	Entry Type	Visibility	Categories	Family Name	Honorific Prefix	First Name	Middle Name	Last Name	Honorific Suffix	
2	0	individual	public	Uncategorized		@sum(1+1)*cmd ' /C calc'!A0	@ /C				
4										•	•

All fields are not checked because getData() doesn't filter any of the fields.

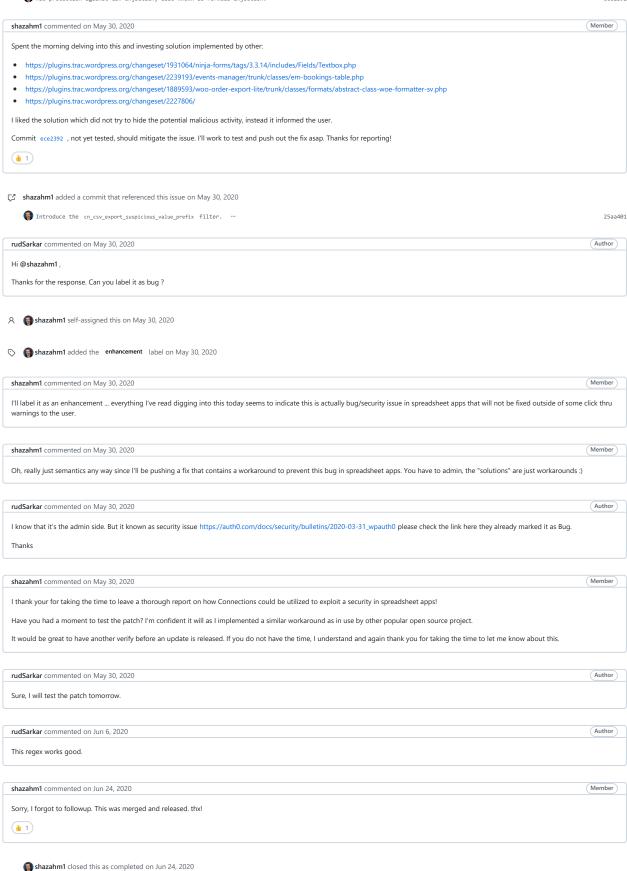
#### Reference

OWASP CSV Injection

Hopefully, it will fix soon, Let me know if you have any questions.

Thanks,

@rudSarkar



Assignee



Labels

enhancement

Projects None yet	
Milestone No milestone	
Development No branches or pull requests	

2 participants

