New issue

Jump to bottom

# Connections 0.7.3.2 <= 9.6 CSV Injection #474

Closed **rudSarkar** opened this issue on May 29, 2020 · 9 comments

Assignees

Labels enhancement

**rudSarkar** commented on May 29, 2020

## Description

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`
5. It will download a file `cn-export-all-MM-DD-YYYY.csv` open it with `Microsoft Excel`
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 | @sum(1+1)*cmd\|' /C calc'!A0 | @sum(1+1)*cmd\|' /C calc'!A0 | @sum(1+1)*cmd\|' /C calc'!A0 | @sum(1+1)*cmd\|' /C calc'!A0 | @ /C |

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

Connections/includes/export/class.csv-export-batch-all.php
Lines 758 to 788 in c69ea8d

```
		public function getData() {

			/** @var wpdb $wpdb */
			global $wpdb;

			$offset = $this->limit * ( $this->step - 1 );

			//if ( 2 <= $this->step ) return FALSE;

			$sql = $wpdb->prepare(
				'SELECT SQL_CALC_FOUND_ROWS *
				 FROM ' . CN_ENTRY_TABLE . '
```

## Reference

> OWASP CSV Injection

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

Thanks,
@rudSarkar

**shazahm1** added a commit that referenced this issue on May 30, 2020

`Add protection against CSV Injection, also known as Formula Injection.` ··· ece2392

**shazahm1** commented on May 30, 2020 Member

Spent the morning delving into this and investing solution implemented by other:

- https://plugins.trac.wordpress.org/changeset/1931064/ninja-forms/tags/3.3.14/includes/Fields/Textbox.php
- https://plugins.trac.wordpress.org/changeset/2239193/events-manager/trunk/classes/em-bookings-table.php
- https://plugins.trac.wordpress.org/changeset/1889593/woo-order-export-lite/trunk/classes/formats/abstract-class-woe-formatter-sv.php
- https://plugins.trac.wordpress.org/changeset/2227806/

I liked the solution which did not try to hide the potential malicious activity, instead it informed the user.

Commit `ece2392` , not yet tested, should mitigate the issue. I'll work to test and push out the fix asap. Thanks for reporting!

👍 1

**shazahm1** added a commit that referenced this issue on May 30, 2020

`Introduce the cn_csv_export_suspicious_value_prefix filter.` ··· 25aa401

**rudSarkar** commented on May 30, 2020 Author

Hi @shazahm1 ,

Thanks for the response. Can you label it as bug ?

**shazahm1** self-assigned this on May 30, 2020

**shazahm1** added the **enhancement** label on May 30, 2020

**shazahm1** commented on May 30, 2020 Member

I'll label it as an enhancement ... everything I've read digging into this today seems to indicate this is actually bug/security issue in spreadsheet apps that will not be fixed outside of some click thru warnings to the user.

**shazahm1** commented on May 30, 2020 Member

Oh, really just semantics any way since I'll be pushing a fix that contains a workaround to prevent this bug in spreadsheet apps. You have to admin, the "solutions" are just workarounds :)

**rudSarkar** commented on May 30, 2020 Author

I know that it's the admin side. But it known as security issue https://auth0.com/docs/security/bulletins/2020-03-31_wpauth0 please check the link here they already marked it as Bug.

Thanks

**shazahm1** commented on May 30, 2020 Member

I thank your for taking the time to leave a thorough report on how Connections could be utilized to exploit a security in spreadsheet apps!

Have you had a moment to test the patch? I'm confident it will as I implemented a similar workaround as in use by other popular open source project.

It would be great to have another verify before an update is released. If you do not have the time, I understand and again thank you for taking the time to let me know about this.

**rudSarkar** commented on May 30, 2020 Author

Sure, I will test the patch tomorrow.

**rudSarkar** commented on Jun 6, 2020 Author

This regex works good.

**shazahm1** commented on Jun 24, 2020 Member

Sorry, I forgot to followup. This was merged and released. thx!

👍 1

**shazahm1** closed this as completed on Jun 24, 2020

Assignees

shazahm1

Labels

**enhancement**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants