CVE-2020-22277 Details

Description:
Import and export users and customers WordPress Plugin through 1.15.5.11 allows CSV injection via a customer's profile.

Additional Information:
In "Import and export users and customers" WordpressPlugin an attacker can register as a user and update hisprofile's info with malicious CSV commands (such as =cmd|'/Cping -t 127.0.0.1'!A0). After that, when the systemadministrator generate CSV output from the systeminformation, there is no check on this inputs and the codesare executable.

Vulnerability Type:
CSV injection

Vendor of Product:
https://codection.com/

Affected Product Code Base:
Import and export users and customers WordpressPlugin 1.15.5.11

Attack Type:
Remote.

Impact:
Code execution.

Discovered By:
Mohamad Pishdar -Web security specialist in Imam Khomeini International University Cert Center (cert.ikiu.ac.ir)-IRAN.

How to Prevent:

To fix this vulnerability, the following points are proposed:

If you have access to new and secure version of Import and export users and customers Wordpress Plugin, be sure to use it:

Official Website

If for any reason you can't update, follow these instructions:

- If you are a programmer, reject any input values that start with: **+, -, =,** and @ (i.e. spreadsheet meta-characters). If need to accept these characters, the application must encode any cell values that interpreted as formulae. This will interpret the entries as data.

- If you are unfamiliar with programming, follow these instructions:
  - Open the CSV output very carefully when starting inputs with some special characters (entries starting with **+, -, =,** and @ i.e. spreadsheet meta-characters).
  - When opening the CSV output in your operating system, notice the alert messages of software (software usually asks you to execute formulas.)
  - Always have a backup of your system.