CVE-2020-22275 Details

Description:

Easy Registration Forms (ER Forms) Wordpress Plugin through 2.0.6 allows CSV injection via ExportSection

Additional Information:

Easy Registration Forms (ER Forms) Wordpress Plugin 2.0.6 allows an attacker to submit an entry with malicious CSV commands (such as =cmd|'/C ping -t 127.0.0.1'!A0). After that, when the system administrator generates CSV output from the forms information, there is no check on this inputs and the codes are executable.

Vulnerability Type:

CSV injection

Vendor of Product:

https://www.easyregistrationforms.com/

Affected Product Code Base:

Easy Registration Forms Wordpress Plugin 2.0.6

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 Easy Registration Forms 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.