CVE-2020-22278 Details

Description:

phpmyadmin through 5.0.2 allows CSV injection via ExportSection

Additional Information:

In phpmyadmin (5.0.2 and fewer than) a attacker cansubmit Malicious CSV Commands on database with related webapp. After that, when the system administrator generate CSVoutput from the database information, there is no check onthis inputs and the codes are executable.

Vulnerability Type:

CSV injection

Vendor of Product:

https://www.phpmyadmin.net

Affected Product Code Base:

phpmyadmin 5.0.2

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 phpmyadmin, 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.