CVE-2020-22274 Details

Description:
JomSocial (Joomla Social Network Extention) 4.7.6 allowCSV injection via a customer's profile.

Additional Information:
In JomSocial (Joomla Social Network Extention) 4.7.6 anattacker can register as a customer and update his profile'sinfo with malicious CSV commands (such as =cmd|'/C ping -t127.0.0.1'!A0). After that, when the system administratorgenerate CSV output from the Monitor /member Section, thereis no check on this inputs and the codes are executable.

Vulnerability Type:
CSV injection

Vendor of Product:
https://www.jomsocial.com/

Affected Product Code Base:
JomSocial 4.7.6

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 JomSocial, be sure to use it:

JomSocial 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.