

CVE-2020-9017 Details

Description:

LiteCart through 2.2.1 allows CSV injection via a customer's profile.

Additional Information:

In Lite-Cart store management system an attacker can register as a customer and update his profile's info with malicious CSV commands (such as =cmd|/C ping -t 127.0.0.1!A0). After that, when the system administrator generate CSV output from the system information, there is no check on this inputs and the codes are executable.

Google Dork:

intext:"Copyright 2020 My Store. All rights reserved Powered by LiteCart"

Vulnerability Type:

CSV injection

Vendor of Product:

<https://www.litecart.net>

Affected Product Code Base:

LiteCart CMS - 2.2.1 and earlier.

Attack Type:

Remote.

Impact:

Code execution.

Impact:

Escalation of Privileges.

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 LiteCart CMS, be sure to use it:

[LiteCart 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.