ERPGo SaaS 3.9 - CSV Injection

EDB-ID:
51220

CVE:
N/A

EDB Verified: ×

Author:
SAJIBE KANTI

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2023-04-03

Vulnerable App:

```
# Exploit Title: ERPGo SaaS 3.9 - CSV Injection
# Date: 18/01/2023
# Exploit Author: Sajibe Kanti
# Vendor Name: RajodiyaInfotech
# Vendor Homepage: https://rajodiya.com/
# Software Link: https://codecanyon.net/item/erpgo-saas-all-in-one-
business-erp-with-project-account-hrm-crm-pos/33263426
# Version: 3.9
# Tested on: Windows & Live Litespeed Web Server
# Demo Link : https://demo.rajodiya.com/erpgo-saas/login

# Description #

ERPGo is a software as a service (SaaS) platform that is vulnerable to CSV
injection attacks. This type of attack occurs when an attacker is able to
manipulate the data that is imported or exported in a CSV file, in order to
execute malicious code or gain unauthorized access to sensitive
information. This vulnerability can be exploited by an attacker by
injecting specially crafted data into a CSV file, which is then imported
into the ERPGo system. This can potentially allow the attacker to gain
access to sensitive information, such as login credentials or financial
data, or to execute malicious code on the system.

# Proof of Concept (PoC) : Exploit #

1) Go To : https://erpgo.127.0.0.1/ERPGo/register <====| Register New
account
2) Complete the Registration
3) Now Click Accounting System Then Customer
4) Now Add a New Vendors / Click Create
5) Now Add this Payload  in Name : =10+20+cmd|' /C calc'!A0
6) Now Submit This Form
7) Now Download Vendors List as csv
8) Open This CSV File in excel
9) Now a Calculator will open

# Image PoC : Reference Image #

1) Payload Fired: https://prnt.sc/EkKPZiMa6yz8
```

Tags:

Advisory/Source: Link