Open in app Get started

Published in Cybersecurity@ValueLabs

ValueLabs Follow
Aug 23 · 2 min read · Listen

Save

# EspoCRM 7.1.8 is vulnerable to CSV Injection

**Affected Product and Version:** EspoCRM 7.1.8

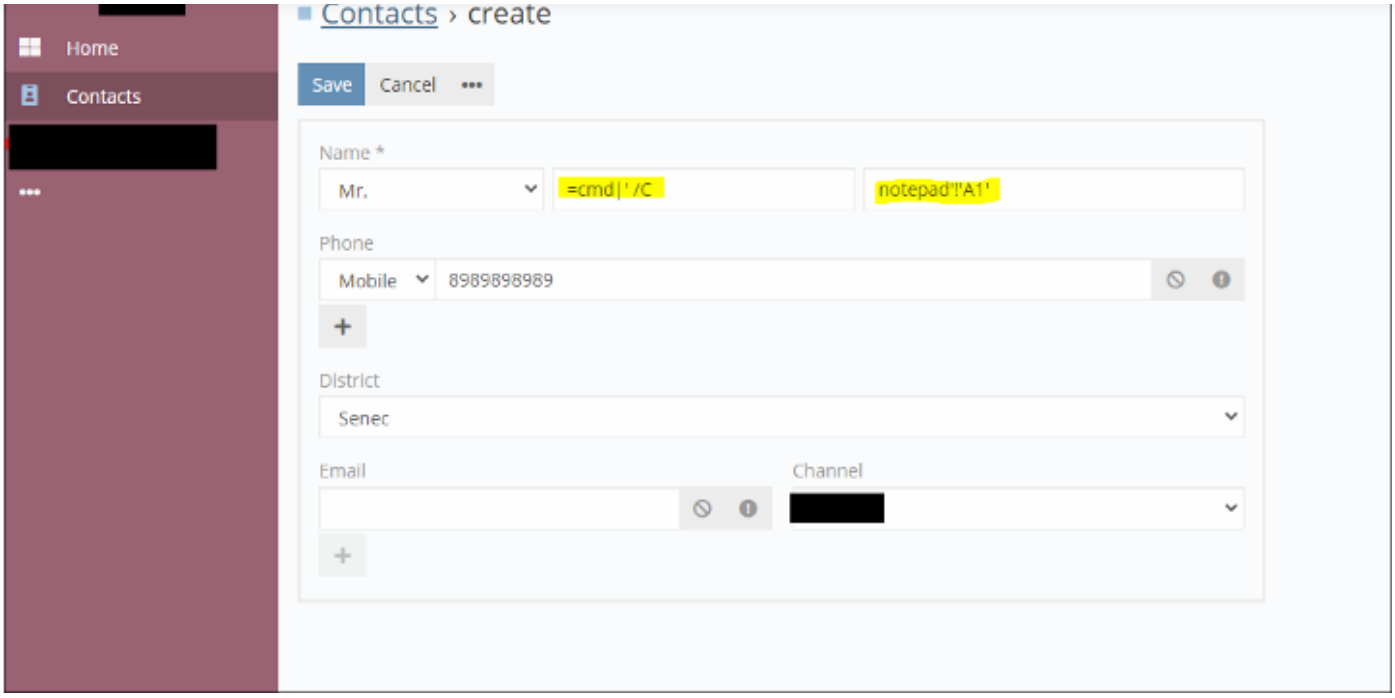
**Description:** EspoCRM is an open-source CRM (customer relationship management) software written in PHP. This web application enables users to see and manage company relationships. EspoCRM version 7.1.8 is vulnerable to CSV injection allowing authenticate users to run system commands on the end user's system by injecting CSV payloads in the input fields while creating contacts and accounts.

**Impact:** There is no direct impact on the application. It depends on the machine/system where the victim tries to open the file. Suppose a malicious CSV file is opened on the machine attached to an organization. In that case, it will allow the attacker to gain access to the device and launch other attacks against the organization.

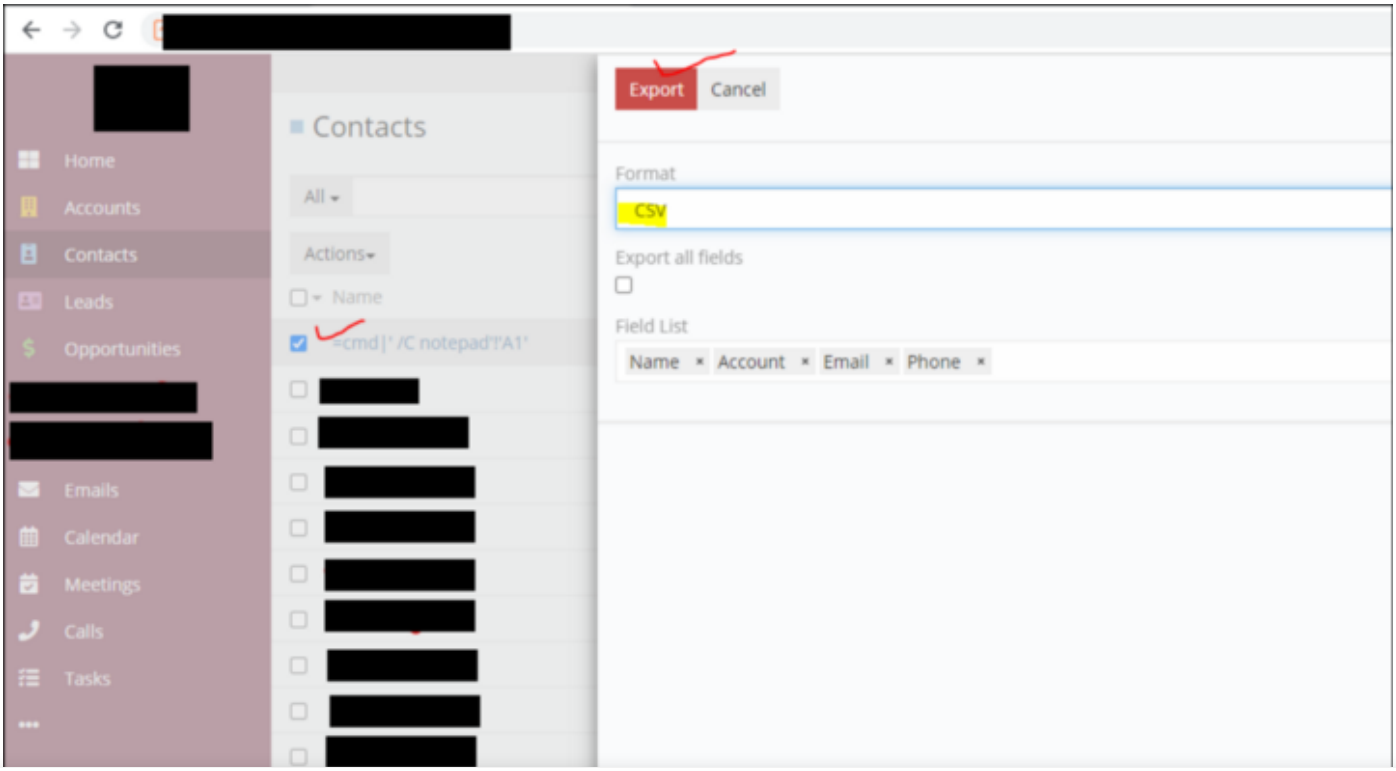
**Steps to reproduce:**

1. Log in to the application as a regular user and navigate to Contacts -> Create Contacts

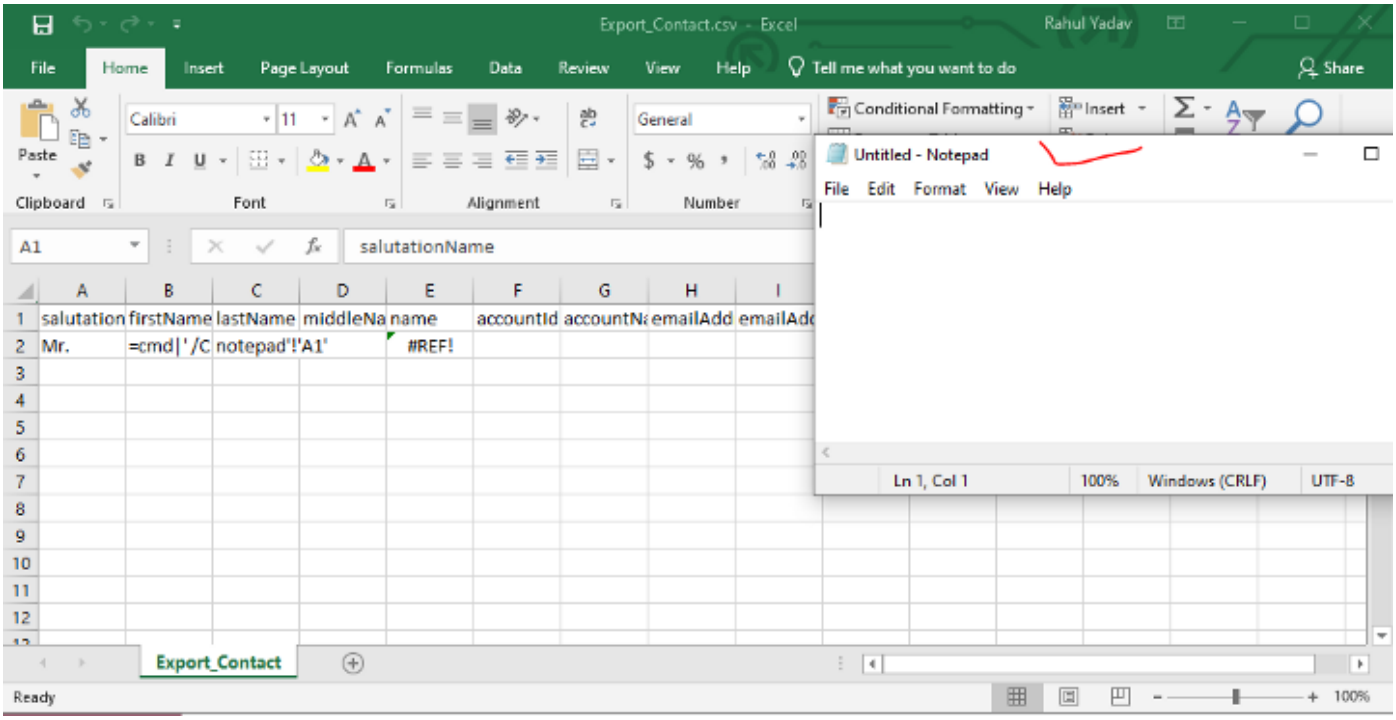
2. Insert a payload (A CSV formula is used as a payload, i.e. [=cmd|'/C notepad'!' A1'] in the first name and last name. Click the save button to create the contact




3. Log in to the application as an administrator (admin user). Navigate to contacts and select the highlighted option. Click export from the actions list. Export the file in CSV format



payloads to run exploits on the end user's machine)




**Note:** More advanced CSV payloads can be used to run other system commands.

**Remediation:**

Update to EspoCRM 7.1.9.

Open in app
Get started