Published in Cybersecurity@ValueLabs

ValueLabs Follow
Aug 23 · 2 min read · Listen

EspoCRM 7.1.8 is vulnerable to Cross Site Scripting

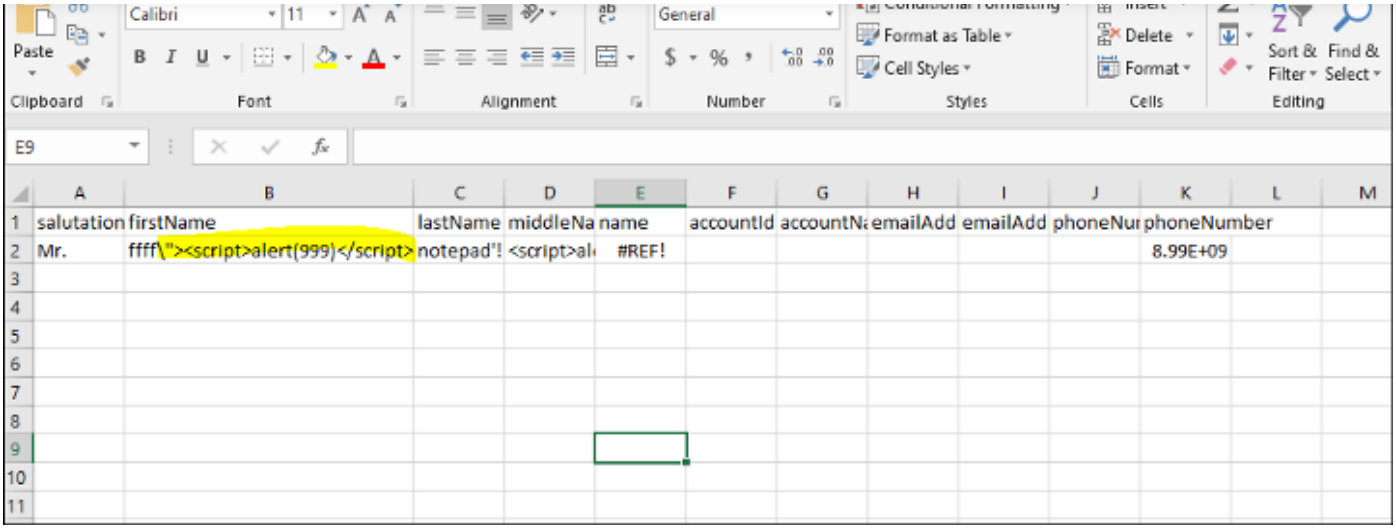
Affected Product and Version: EspoCRM 7.1.8

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 Cross Site Scripting, allowing attackers to run malicious JavaScript on the browser. Administrator users can import contacts through the CSV file. Attackers can craft a CSV file containing JavaScript payloads and send it to the Administrator. JavaScript payload gets executed on import.

Impact: The attacker may access the session ID of the victim and send it to a remote server. Under this situation, the attacker may use this session ID to get control of the Administrator user and perform all the actions an administrator can perform. The attacker can deface the website and steal the credentials of the administrator user.

Steps to reproduce:

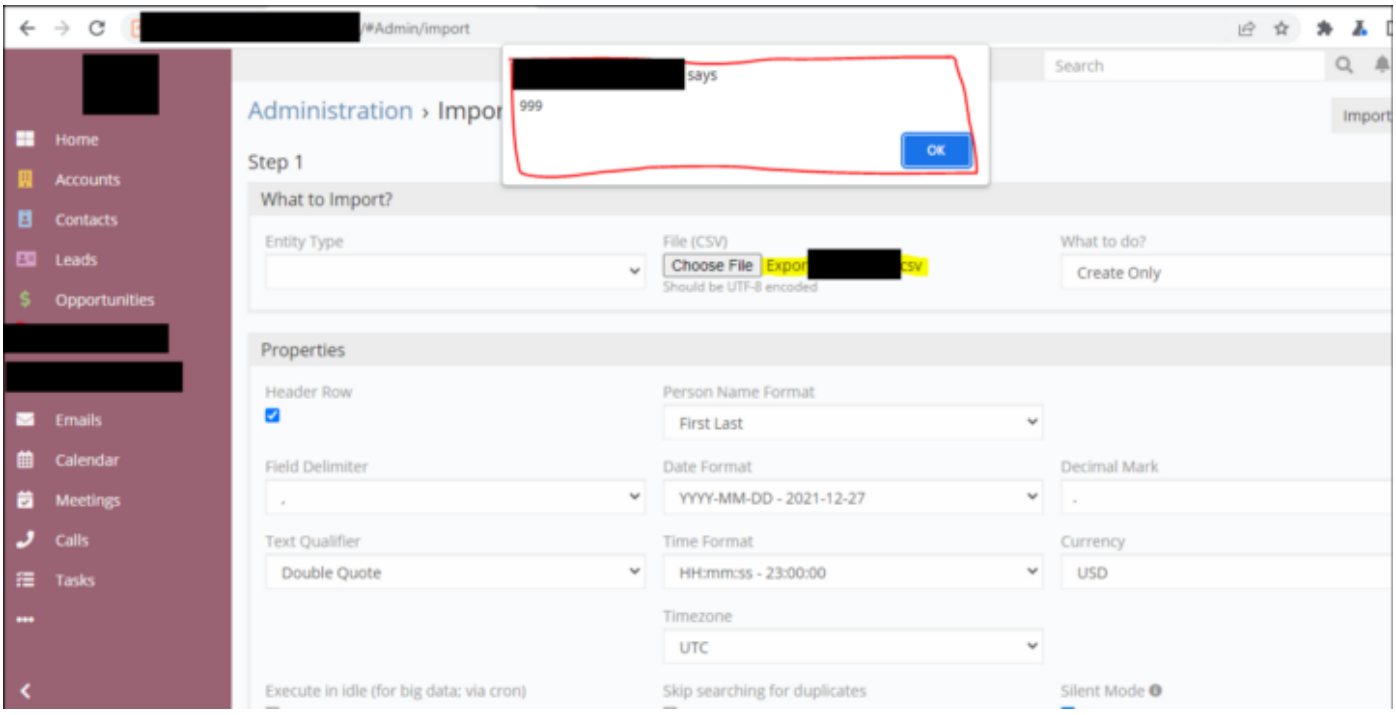
1. Craft a CSV file containing a malicious JavaScript payload

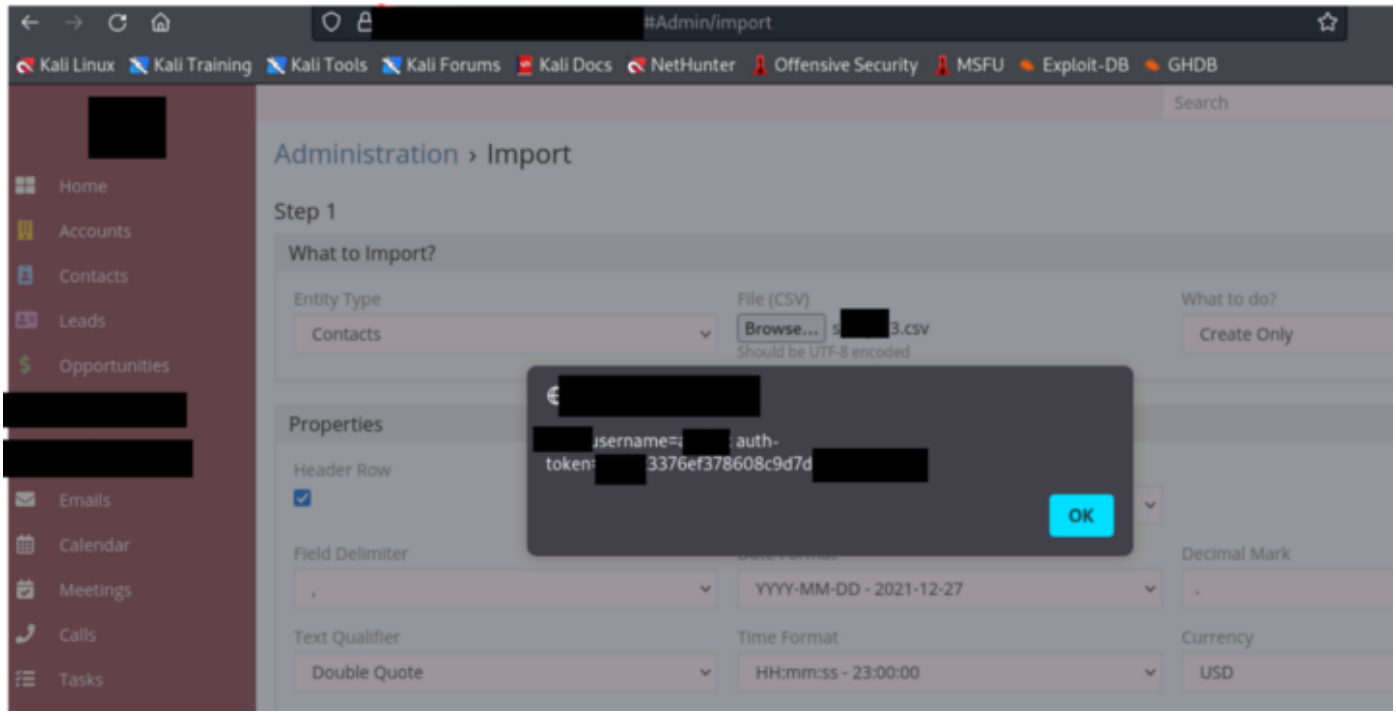


2. Log in to the application as an administrator user. Navigate to Administrator>> Import

3. Click New import and choose the CSV file (as shown in step 1) containing the malicious payload

4. Observe that payload gets executed on the browser





Remediation:

Upgrade to the latest stable version of EspoCRM 7.1.9