Published in Cybersecurity@ValueLabs

ValueLabs Follow
Aug 23 · 1 min read · Listen

EspoCRM 7.1.8 is vulnerable to Missing Secure Flag

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 Missing Secure Flag, allowing the browser to send plain text cookies over an insecure channel (HTTP). The attacker may capture the cookie from the insecure channel using a MITM attack.

Impact: The attacker may use the captured cookie to access the application as an authenticated user and perform actions a genuine user can perform. The impact varies depending on the role of the compromised user.

Steps to reproduce:

1. Log in to the application

2. Capture the response to the login request. Observe that the secure flag is missing

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 16 Jun 2022 14:41:42 GMT
Content-Type: application/json
Connection: close
Set-Cookie: auth-token-secret=2a9614[redacted]d5ee8ce653f; path=/; expires=Wed, 12 Mar 2025 14:41:42 GMT;
HttpOnly; SameSite=Lax
Expires: 0
Last-Modified: Thu, 16 Jun 2022 14:41:42 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 34920

{
  "user":{
    "id":"1",
    "name":"<meta>",
    "deleted":false,
    "userName":"admin",
    "type":"admin",
    "authMethod":null,
    "apiKey":null,
    "salutationName":null,
    "firstName":null,
    "lastName":"<meta>",
    "isActive":true,
    "title":"<b>sample page<\/b>",
    "emailAddress":null,
    "phoneNumber":null,
    "token":"64cc[redacted]73a3bb",
```

Remediation:

Upgrade to the latest stable version of EspoCRM 7.1.9