

[Open in app](#)[Get started](#)

Published in Cybersecurity@ValueLabs



ValueLabs

[Follow](#)

Aug 23 · 1 min read · [Listen](#)

[Save](#)

# 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



[Open in app](#)[Get started](#)

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Thu, 16 Jun 2022 14:41:42 GMT
4 Content-Type: application/json
5 Connection: close
6 Set-Cookie: auth-token-secret=2a9614[REDACTED]d5ee8ce653f; path=/; expires=Wed, 12 Mar 2025 14:41:42 GMT;
  HttpOnly; SameSite=Lax
7 Expires: 0
8 Last-Modified: Thu, 16 Jun 2022 14:41:42 GMT
9 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
10 Pragma: no-cache
11 Content-Length: 34920
12
13 {
  "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

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app





[Open in app](#)

Get started

