Published in Cybersecurity@ValueLabs

ValueLabs Follow
Aug 23 · 1 min read · Listen

Save

EspoCRM 7.1.8 is vulnerable to Unrestricted File Upload

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 Unrestricted File Upload allowing attackers to upload a malicious file with any extension to the server. The attacker may execute these malicious files to run unintended code on the server to compromise the server.

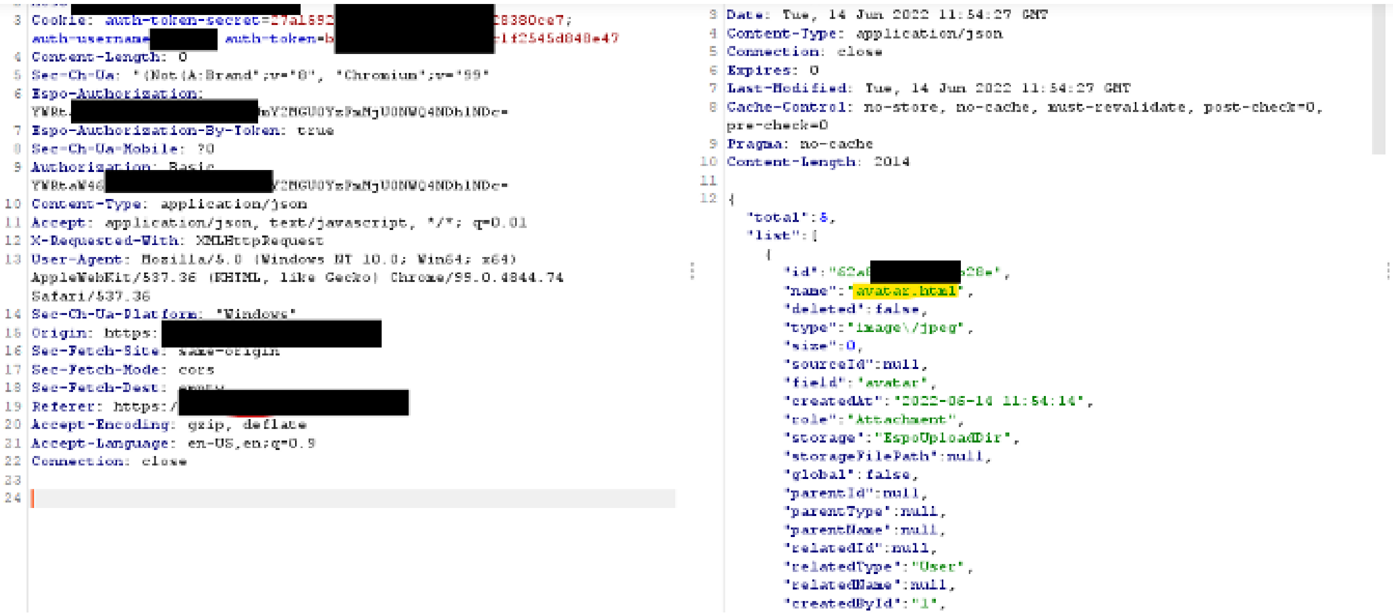
Impact: The attacker may run malicious code on the server and compromise the confidentiality, integrity, and availability of the server and application.

Steps to reproduce:

1. Log in to the application

2. Go to the profile page and upload the file with the HTML extension

3. Access the uploaded file and observe that it gets uploaded successfully



```
Cookie: auth-token-secret=27a1692[redacted]28380ce7;
auth-username=[redacted] auth-token=b1f2545d848e47
Content-Length: 0
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Espo-Authorization:
YWRt[redacted]mY2MGU0YzFmMjU0NWQ4NDh1NDc=
Espo-Authorization-By-Token: true
Sec-Ch-Ua-Mobile: ?0
Authorization: Basic
YWRtaW46[redacted]Y2MGU0YzFmMjU0NWQ4NDh1NDc=
Content-Type: application/json
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https:[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest:
Referer: https:/[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
Date: Tue, 14 Jun 2022 11:54:27 GMT
Content-Type: application/json
Connection: close
Expires: 0
Last-Modified: Tue, 14 Jun 2022 11:54:27 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Length: 2014

{
  "total":5,
  "list":[
    {
      "id":"62a6[redacted]28e",
      "name":"avatar.html",
      "deleted":false,
      "type":"image\/jpeg",
      "size":0,
      "sourceId":null,
      "field":"avatar",
      "createdAt":"2022-06-14 11:54:14",
      "role":"Attachment",
      "storage":"EspoUploadDir",
      "storageFilePath":null,
      "global":false,
      "parentId":null,
      "parentType":null,
      "parentName":null,
      "relatedId":null,
      "relatedType":"User",
      "relatedName":null,
      "createdById":"1",
```

Remediation:

Upgrade to the latest stable version of EspoCRM 7.1.9