

[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 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



1



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

```
3 Cookie: auth-token-secret=7a1592...E8380ce7;
  auth-username=... auth-token=b...-1f2545d048e47
4 Content-Length: 0
5 Sec-Ch-Ua: "(Not:A:Brand";v="0", "Chromium";v="99"
6 Espo-Authentication:
  YWRtcA96...nY2NGU0YzFmMjU0NWQ4NDh1NDc=
7 Espo-Authentication-By-Token: true
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Basic
  YWRtcA96.../Z2NGU0YzFmMjU0NWQ4NDh1NDc=
10 Content-Type: application/json
11 Accept: application/json, text/javascript, */*; q=0.01
12 X-Requested-With: XMLHttpRequest
13 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
14 Sec-Ch-Ua-Platform: "Windows"
15 Origin: https://...
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: document
19 Referer: https://...
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-US,en;q=0.9
22 Connection: close
23
24
```

```
3 Date: Tue, 14 Jun 2022 11:54:27 GMT
4 Content-Type: application/json
5 Connection: close
6 Expires: 0
7 Last-Modified: Tue, 14 Jun 2022 11:54:27 GMT
8 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
  pre-check=0
9 Pragma: no-cache
10 Content-Length: 2014
11
12 {
  "total": 5,
  "list": [
    {
      "id": "62a...28",
      "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

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

Get the Medium app



