CYBERPEACE

SECURITY ADVISORY

Advisory Report on NVIDIA D3D10 Driver Bugs Vulnerability

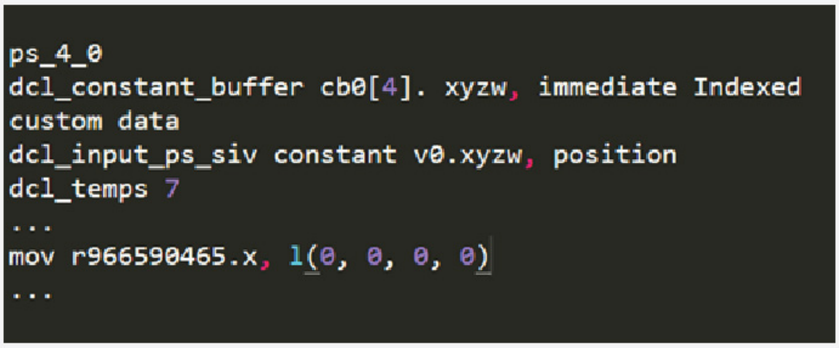
Problem Name/ID: NVIDIA D3D10 Driver Bugs Vulnerability

Severity: Medium to High

Executive Summary:

Security updates to represent high severity vulnerabilities in Windows Graphics Processing Unit(G-PU) display drivers that lead to remote code execution(RCE),escalation of privileges(action of introducing the bug into an operating system),information disclosure(application fails to protect sensitive information properly through which important information get leaked) and Dos attack(Shutting down a machine without the knowledge of the user). The GPU display drivers failure which impacted the window machine as a risk assessment based on the average risk across a device. Multiple remote code execution(REC) vulnerabilities were identified in the **NVIDIA D3D10** driver. This driver supports multiple **Graphical User Interface (GUI)**. This vulnerability supplies the user with a faulty shader, forcefully allowing them to introduce malicious code on the victim's machine.These bugs allow attackers to perform **virtual machine escape** i.e. to give access to the attackers to escape the virtual machine and gain access to the indicated operating system which is a so-called **guest-to-host escape**. Initially, the vulnerability was indicated when the user updated the driver and after installing the update the system of the victim started compromising. **Common Vulnerability Exposure** 2020-5981 NVIDIA D3D10 driver that contains malware in the user mode driver (**nvwg f2um/x.dll**) in which processing in the library of the driver in which graphics lead to memory corruption vulnerability. Below are some of the vulnerability related to the above driver as
nvwgf2umx_cfg.dll nvwg MOV code execution vulnerability:

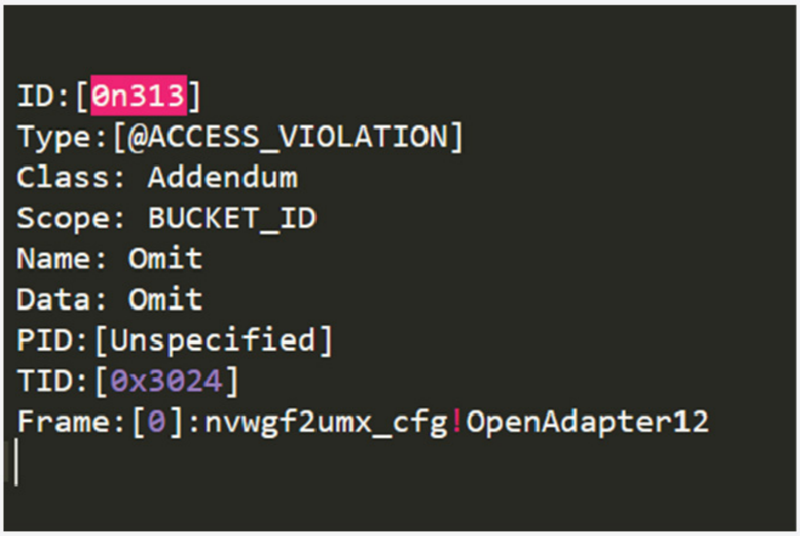
An exploitable code execution vulnerability in nvwg MOV functionality of NVIDIA D3D10 driver existed in version of **442.50-26.21.14.4250**. A specially crafted shader that causes remote code execution using the same guest-to-host escape method. NVIDIA Graphic drivers are software which communicates between Operating System and GPU devices. For example, a code which triggered the pixel:



```
ps_4_0
dcl_constant_buffer cb0[4]. xyzw, immediate Indexed
custom data
dcl_input_ps_siv constant v0.xyzw, position
dcl_temps 7
...
mov r966590465.x, l(0, 0, 0, 0)
...
```

The remote code execution vulnerability was triggered by supplying a malformed pixel shader which leads to memory corruption. In this process, **attackers control the destination address by modifying the shader code**. The installed file was rdvgm.exe like Hyper-V which is a platform to run multiple Operating Systems in one system.

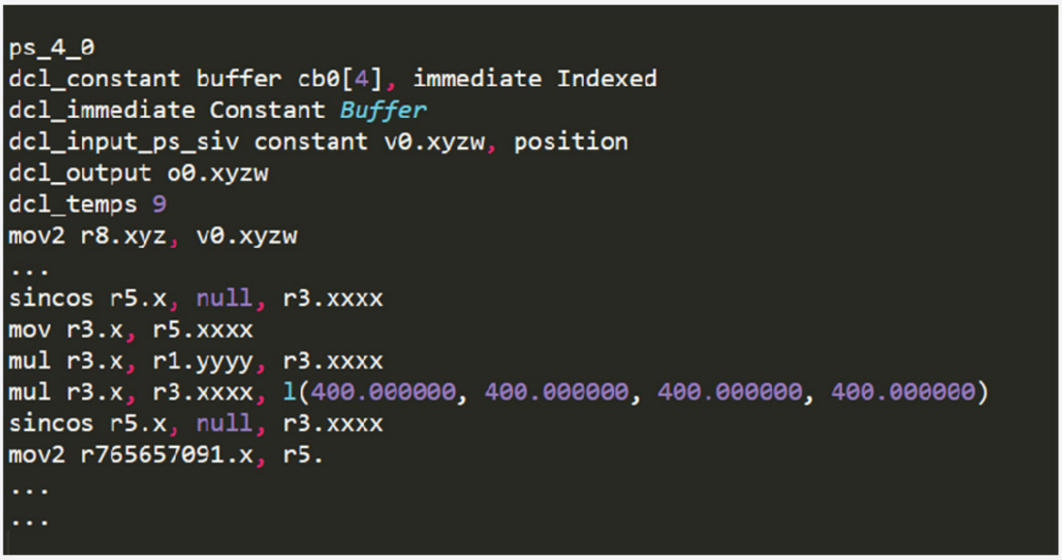
Some ID's related to the above vulnerability :



```
ID:[0n313]
Type:[@ACCESS_VIOLATION]
Class: Addendum
Scope: BUCKET_ID
Name: Omit
Data: Omit
PID:[Unspecified]
TID:[0x3024]
Frame:[0]:nvwgf2umx_cfg!OpenAdapter12
```

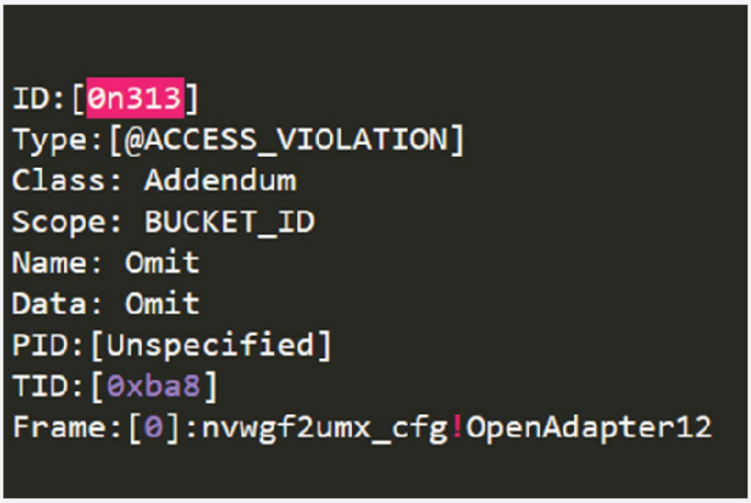
nvwgf2umx_cfg.dll nvwg MOV2 code execution vulnerability:

Similar to the above vulnerability but a slight code change was made. The code below in which by modifying the MOV destination register operand in the mov2(A quick Time File Format Application) intrusion an attacker able to trigger memory corruption vulnerability in the NVIDIA graphic driver. In this process, attackers can partially control the destination address.



```
ps_4_0
dcl_constant buffer cb0[4], immediate Indexed
dcl_immediate Constant Buffer
dcl_input_ps_siv constant v0.xyzw, position
dcl_output o0.xyzw
dcl_temps 9
mov2 r8.xyz, v0.xyzw
...
sincos r5.x, null, r3.xxxx
mov r3.x, r5.xxxx
mul r3.x, r1.yyyy, r3.xxxx
mul r3.x, r3.xxxx, l(400.000000, 400.000000, 400.000000, 400.000000)
sincos r5.x, null, r3.xxxx
mov2 r765657091.x, r5.
...
...
```

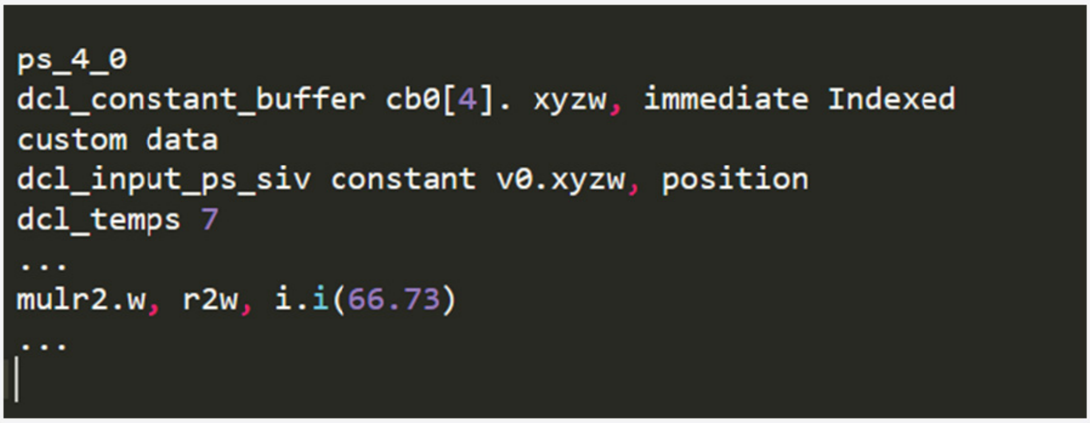
ID's related to this vulnerability:



```
ID:[0n313]
Type:[@ACCESS_VIOLATION]
Class: Addendum
Scope: BUCKET_ID
Name: Omit
Data: Omit
PID:[Unspecified]
TID:[0xba8]
Frame:[0]:nvwgf2umx_cfg!OpenAdapter12
```

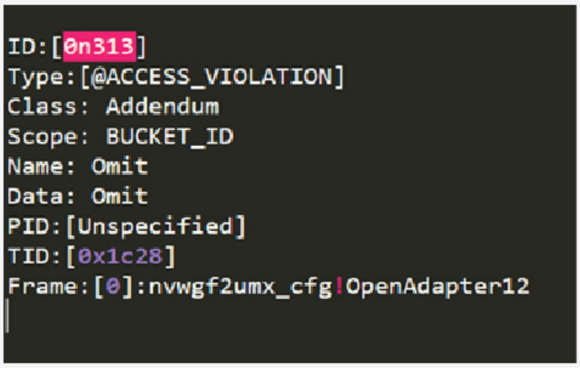
nvwgf2umx_cfg.dll nvwg MUL code execution vulnerability:

An exploitable code exists in nvwg MUL functionality of the NVIDIA D3D10 driver. In this by modifying intrusion code mulr2.w, r2w, i.i(66.73) to the registration number; MUL r-2048691710w, r2.w; 1(66.73) it is possible to trigger a memory corruption vulnerability in the driver.



```
ps_4_0
dcl_constant_buffer cb0[4]. xyzw, immediate Indexed
custom data
dcl_input_ps_siv constant v0.xyzw, position
dcl_temps 7
...
mulr2.w, r2w, i.i(66.73)
...
```

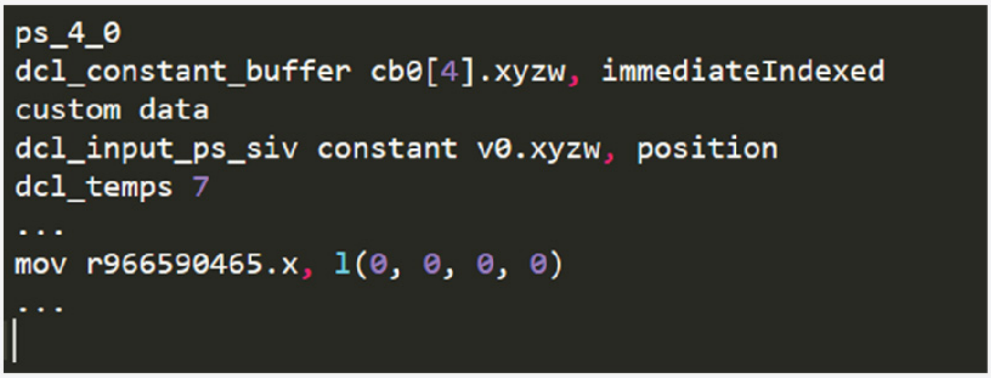
The ID’s related to this vulnerability are :



```
ID:[0n313]
Type:[@ACCESS_VIOLATION]
Class: Addendum
Scope: BUCKET_ID
Name: Omit
Data: Omit
PID:[Unspecified]
TID:[0x1c28]
Frame:[0]:nvwgf2umx_cfg!OpenAdapter12
```

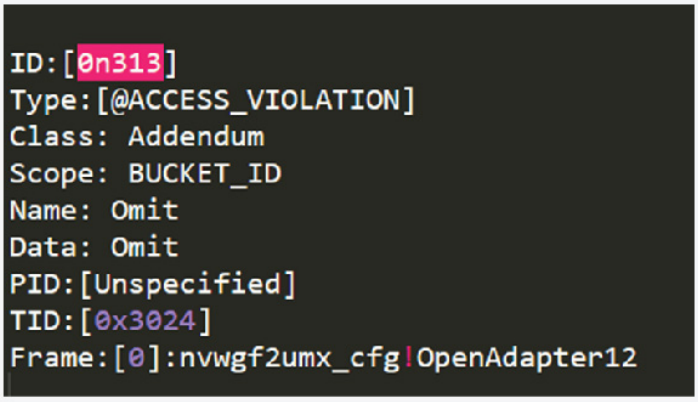
nvwgf2umx_cfg.dll nvwg MOV code execution vulnerability (Constant Buffer):

Vulnerability in nvwy DCL-CONSTANT BUFFER functionality of NVIDIA driver of the same version in which functionality is the same as stated above. Code related to this vulnerability:



```
ps_4_0
dcl_constant_buffer cb0[4].xyzw, immediateIndexed
custom data
dcl_input_ps_siv constant v0.xyzw, position
dcl_temps 7
...
mov r966590465.x, l(0, 0, 0, 0)
...
```

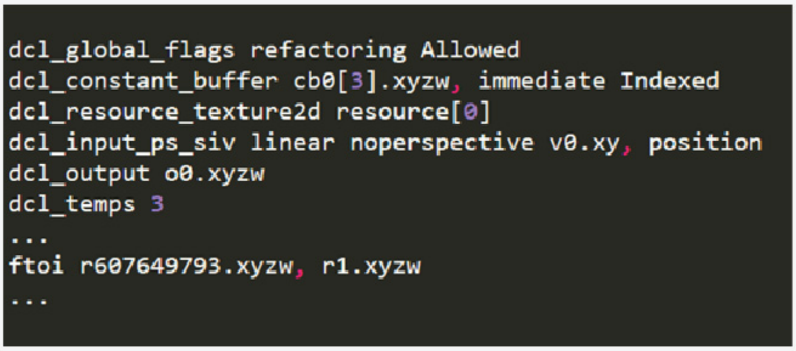
ID's related to the above vulnerability :



```
ID:[0n313]
Type:[@ACCESS_VIOLATION]
Class: Addendum
Scope: BUCKET_ID
Name: Omit
Data: Omit
PID:[Unspecified]
TID:[0x3024]
Frame:[0]:nvwgf2umx_cfg!OpenAdapter12
```

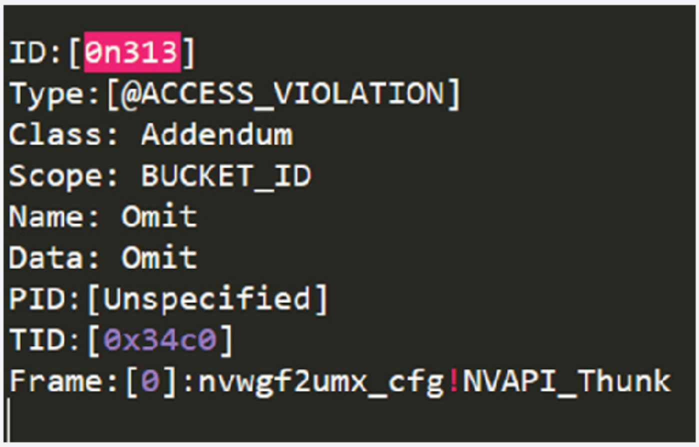
nvwgf2umx_cfg.dll nvwg FTOI code execution vulnerability:

Vulnerable code was executed in the driver file nvwgf2umx.cfy.dll, in this, modifying the ftoi (floating point to signed integer conversion) destination to a value of the typical register number which was possible for an attacker to trigger a memory corruption vulnerability in the driver. In this process, the attacker controls the destination address by changing the operand value in the code. Code relate to this



```
dcl_global_flags refactoring Allowed
dcl_constant_buffer cb0[3].xyzw, immediate Indexed
dcl_resource_texture2d resource[0]
dcl_input_ps_siv linear noperspective v0.xy, position
dcl_output o0.xyzw
dcl_temps 3
...
ftoi r607649793.xyzw, r1.xyzw
...
```

Problem IDs related to above vulnerability :



```
ID:[0n313]
Type:[@ACCESS_VIOLATION]
Class: Addendum
Scope: BUCKET_ID
Name: Omit
Data: Omit
PID:[Unspecified]
TID:[0x34c0]
Frame:[0]:nvwgf2umx_cfg!NVAPI_Thunk
```

IOC Related to above vulnerabilities

> NVIDIA D3D10 driver nvwgf2umx_cfg.dll nvwg MOV code execution vulnerability:

- HASH: 07cf5b1cb3db334c45e135329df89c5b430e148b
- SHA1_HASH: 0bb9b3455134f525fc8cb50a235016bcdddd1bc9
- SHA1_HASH_MOD_FUNC: cf11ca47cd244828b4bd54f41d1a85654a927900
- SHA1_HASH_MOD_FUNC_OFFSET: 2faf18a98d1c68b5746888e583c56af549c3d318
- SHA1_HASH_MOD: 701c05ef09dbf52b13a73d3e2d555e4906a8342
- URL:http://watson.microsoft.com/StageOne/rdvgm.ex-e/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030cecf.htm?Retriage=1
- Bit Defender: computer and software
- Comodo Valkyrie Verdict media sharing
- Forcepoint: Threat Seeker information technology
- sophos: information technology
- HTTP Response
- FinalURL:http://watson.microsoft.com/StageOne/rdvgm.ex-e/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030cecf.htm?Retriage=1
- Serving IP Address:52.255.148.73
- IP:52.255.148.73
- Hostname:52.255.148.73
- ASN:8075
- ISP:Microsoft Corporation
- Organization:Microsoft Azure
- Services:None detected
- Continent:North America
- Country:United States
- State/Region:Virginia
- City:Washington
- FAILURE_ID_HASH:32968bfd-cb9d-86c1-30b8-ad1954eb9190

> NVIDIA D3D10 driver nvwgf2umx_cfg.dll nvwg MOV2 code execution vulnerability:

- HASH: 633b95c9e05d81568106c5eb6d754c627031543d
- SHA1_HASH: 87cb7fbfa77a2f9cc0c73fea9f9a68d4ae0be36e:
- SHA1_HASH_MOD_FUNC_OFFSET:33ebce64065a7eab7e4ea78fdccda28a11a5bae1:
- SHA1_HASH_MOD: 701c05ef09dbf52b13a73d3e2d555e4906a8342a:
- URL:http://watson.microsoft.com/StageOne/rdvgm.exe/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030cf90.htm?Retriage=1
- Bit Defender: computer and software
- Comodo: Valkyrie Verdict media sharing
- Forcepoint ThreatSeeker information technology
- Sophos: information technology
- FinalURL:http://watson.microsoft.com/StageOne/rdvgm.exe/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030cf90.htm?Retriage=1
- Serving IP Address:52.255.148.73
- IP:52.255.148.73
- Hostname:52.255.148.73
- ASN:8075
- Services: None detected
- Continent: North America
- Country: United States
- State/Region:Virginia
- City: Washington

> NVIDIA D3D10 driver nvwgf2umx_cfg.dll nvwg MUL code execution vulnerability:

- HASH:622081de292639ef2eb530c827e84fc0b54d4fa4:
- SHA1_HASH:066d72a0d47d3b063c2d64e78e469c18b0411eb3:
- SHA1_HASH_MOD_FUNC:8016138a2a39cc33d8dac8a84b1c2a1effc346be:
- SHA1_HASH_MOD_FUNC_OFFSET:8554a8cb2835306423b02b0892307f8eca51ea16:
- SHA1_HASH_MOD: 003810612d6ab3b00a71ed5b91e0c10272be87ae:
- URL:http://watson.microsoft.com/StageOne/rdvgm.exe/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030dff8.htm?Retriage=1
- Bit Defender: computer and software
- Forcepoint: Threat Seeker information technology
- Sophos: information technology
- FinalURLhttp://watson.microsoft.com/StageOne/rdvgm.exe/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030dff8.htm?Retriage=1

- Serving IP Address:13.88.21.125
- Hostname:13.88.21.125
- Organization: Microsoft Azure
- Services: None detected
- Continent: North America
- Country: United States
- State/Region:California
- City: San Jose

> NVIDIA D3D10 Driver nvwgf2umx_cfg.dll nvwg FTOI code execution vulnerability:

- HASH: c7265071fb60e87a75898e3ea660ed9a1a6dd1c8:
- HASH: 0f361cbbe04384b6e38c75ba58473fb3acfe310b:
- HASH_MOD_FUNC:93c9ea155a8ea6b1efda165d582f312e74a6054c:
- HASH_MOD_FUNC_OFFSET: dfebc1d571830737fa18e4248bead5bad25adf26:
- HASH_MOD: 685fcebdc54c161cffb3ee49c08a2ea54c68ef8d:
- HASH: fd06a8b6-fe43-abcd-e2a7-ab697f9fc3df:
- URL:http://watson.microsoft.com/StageOne/rdvgm.ex-e/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030cecf.htm?Retriage=1
- Bit Defender: computer and software
- Forcepoint: Threat Seeker information technology
- Sophos: information technology
- FinalURL:http://watson.microsoft.com/StageOne/rdvgm.ex-e/10.0.18362.693/c2ed11f1/nvwgf2umx_cfg.dll/26.21.14.4250/5e543369/c0000005/0030cecf.htm?Retriage=1
- Serving IP Address:13.88.21.125
- Hostname:13.88.21.125
- ASN:8075
- ISP: Microsoft Corporation
- Organization: Microsoft Azure
- Services: None detected
- Continent: North America
- Country: United States
- State/Region:California
- City: San Jose

Recommendation:

- Patch the system with official security updates and verify after the update and install. Use the official website for any updates for drivers and others. Don't update the system and drivers unwantedly or when it is not required. It is suggested to download drivers from official websites only not from any 3rd party websites.
- After updating drivers once, check-in the library folder, the file is added, or deleted from the folder or not.

Reference:

1. https://www.bleepingcomputer.com/news/security/nvidia-fixes-high-severity-flaws-in-windows-display-driver/
2. https://blog.talosintelligence.com/2020/09/vuln-spotlight-nvidia-d3d10-.html?m=1
3. https://www.helpnetsecurity.com/2018/11/07/virtualbox-guest-to-host-escape-0day/
4. https://talosintelligence.com/vulnerability_reports/TALOS-2020-1035
5. https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/
6. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5981
7. https://talosintelligence.com/vulnerability_reports/TALOS-2020-1037
8. https://phishing.ws/index.php/2020/10/03/cve-2020-5981/

Revision Notes:

Version	Description	Section	Status	Date
1.0	Initial Public Release	---	Final	17/10/2020

Issued by

Research Wing, CyberPeace Foundation

CYBERPEACE

www.cyberpeace.org | secretariat@cyberpeace.net

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation