Win32k elevation of privilege vulnerability

(Win32k ConsoleControl Offset Confusion)

CVE-2021-1732

Ratnayake T.D  
Faculty of Computing *Sri Lanka Institute of Information*   
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 4th Given Name Surname  
line 2: *dept. name of organization*  
*(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCIDline 1: 2nd Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 5th Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCIDline 1: 3rd Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 6th Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

*Abstract*—

This paper describes our first research experience in the win32k elevation of privilege vulnerability

Keywords—component, formatting, style, styling, insert (key words)

# Introduction

CVE-2021-1732 is a win32k window object type confusion vulnerability that results in an OOB (out-of-bounds) write that can be leveraged to establish arbitrary memory read and write capabilities within the Windows kernel (local Elevation of Privilege (EoP)). To get beyond recent attack mitigations like DEP, ASLR, and CFG on hardened operating systems like Windows 10, memory exploitation usually requires a read, write, and execute primitive. Because it does not seek to execute malicious code in memory, a data-only attack only requires a read and write primitive. Instead, it manipulates data structures utilized by the operating system to its advantage (i.e., to achieve elevated privileges).[1]

**Win32k**

The Graphics Device Interface allows graphical content to be delivered to displays, printers, and other output devices. In user mode, it is found in gdi.exe on 16-bit Windows and gdi32.dll on 32-bit Windows. Kernel-mode Win32k.sys, which talks directly with the graphics driver, provides GDI support.

**LPE**

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

**CVE-2021-1732**

Permits an attacker to try to exploit a Microsoft Windows Win32K privilege escalation (EOP) vulnerability. A remote attacker may be able to take advantage of this to get access to susceptible systems. The attacker must have active session access to the target machine to exploit this vulnerability. A boundary mistake in the Win32k.sys driver in the Windows kernel causes the vulnerability. A local user can use a specially written software to cause memory corruption and execute arbitrary code with elevated privileges on the system.[2]

# Background / Literature Survey

Win32k is a graphical (GUI) component of the Microsoft Windows Subsystem, with the majority of its code running in the kernel for performance. It's used to print the Windows OS desktop in graphical format. Due to the win32k design, the kernel component of win32k must still be able to call user mode via user-mode callback methods in order to ease window creation and management.

1. The flaw exists in the "win32kfull!NtUserCreateWindowEx" Windows graphics driver.
2. When the driver win32kfull.sys uses "NtUserCreateWindowEx" to construct a window, tagWND => cbWndExtra (the amount of extra memory allocated by the window instance) is checked. When the value is not empty, it uses the "win32kfull!xxxClientAllocWindowClassExtraBytes" function to call back the user layer "user32.dll! xxxClientAllocWindowClassExtraBytes" to allocate memory, then uses the "NtCallbackReturn function" to correct the stack before returning to the kernel layer, saving and continuing to run. When the 0x800 attribute is present in the tagWND => flag value, the value is addressed with an offset.

##### Acknowledgment *(Heading 5)*

##### References

1. Eoin Carroll , “[Technical Analysis of CVE-2021-1732](https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/technical-analysis-of-cve-2021-1732/)”, January 05,2022..
2. Palo Alto , “[Win32k elevation of privilege vulnerability](https://www.safe.security/assets/img/research-paper/pdf/windows-win32k-elevation-of-privilege-vulnerability.pdf)” , 2021.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.**