**Windows Win32k**

**Permission enhancement vulnerability**

**(CVE-2023-29336)**

**Deep analysis report**

**Catalogue**

[1. Basic information 1](#_Toc137826603)

[2. Threat assessment 2](#_Toc137826604)

[3. The security status of the affected assets 2](#_Toc137826605)

[4. Disposal advice 3](#_Toc137826606)

[5. The full utilization process 3](#_Toc137826607)

[6. Use of monitoring and protection 9](#_Toc137826608)

1.Basic information

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability name** | **Windows Win32k, Authority promotion vulnerability** | | |
| **Open time** | 2023-05-09 | **refresh time** | 2023-06-16 |
| **CVE number** | CVE-2023-29336 |
| **Threat type** | Code execution | **Technology type** | Reuse after release |
| **Manufacturer name** | Microsoft | **Product name** | Windows |
| **Real threat state** | | | |
| **POC state** | **EXP state** | **Use state in the field** | **Technical detail status** |
| **publiced** | **publiced** | **Has been found** | **publiced** |
| **Vulnerability description** | Win32k. The sys is a core system file of the Windows operating system, which is part of the Win32 API to handle graphical user interface (GUI) related tasks. Win32k.sys mainly provides a set of graphics device interface (GDI) and user interface (UI) related APIs, including window management, messaging, drawing and font processing functions.  Win32k There is a post-release reuse vulnerability in Win32k. An authenticated local attacker can construct malicious programs to trigger the vulnerability. Successful exploitation of this vulnerability can increase permission to SYSTEM or cause system crash. | | |
| **Influence version** | Windows Server 2012 R2 (Server Core installation)  Windows Server 2012 R2  Windows Server 2012 (Server Core installation)  Windows Server 2012  Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)  Windows Server 2008 R2 for x64-based Systems Service Pack 1  Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)  Windows Server 2008 for x64-based Systems Service Pack 2  Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)  Windows Server 2008 for 32-bit Systems Service Pack 2  Windows Server 2016 (Server Core installation)  Windows Server 2016  Windows 10 Version 1607 for x64-based Systems  Windows 10 Version 1607 for 32-bit Systems  Windows 10 for x64-based Systems  Windows 10 for 32-bit Systems | | |
| **Other affected components** | None | | |

2. Threat assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CVSS 3.1 Rating** | **high risk** | **The CVSS 3.1 Score** | | 7.8 |
| **CVSS vector** | **Access route (AV)** | | **Attack complexity (AC)** | |
| this locality | | low | |
| **Required permission (PR)** | | **User Interaction (UI)** | |
| low | | non-essential | |
| **incidence (S)** | | **Confidentiality Impact (C)** | |
| no change | | high | |
| **Integrity Impact (I)** | | **Availability Effects (A)** | |
| high | | high | |
| **Hazard description** | An authenticated local attacker can construct a malicious program to trigger the vulnerability, and the vulnerability can increase the permission to SYSTEM or cause a system crash. | | | |

3. The security status of the affected assets

Not available

4. Disposal advice

|  |  |  |
| --- | --- | --- |
| **Self-examination and testing scheme** | 1. Pass version detection (recommended update to latest version)   2, by PoC | |
| **Automated vulnerability scanning method** | Not available | |
| **Repair mitigation measures** | Please keep automatic updates enabled, or refer to the following link to upgrade to the secure version: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336 | |
| **Repair solution (including vulnerability patches)** | Microsoft has now released a security update, and users can obtain it through the Windows update. If the update cannot be updated automatically, please refer to the following link to download and install the corresponding version of the security patch:  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336 | |
| **The effects of the repair caused** | Whether the operating system is required to be restarted | yes |
| Need to restart the application system | deny |
| other |  |

5. The full utilization process

|  |  |
| --- | --- |
| **EXP/POC** | See the attachment for the PoC. |
| **Use details to describe** | With the patch diff, vulnerabilities can be found in xxxEnableMenuItem  Because the win 32k component on the Windows exists for a long time, the leaked source code of its earlier version can be searched through the Internet.xxxEnableMenuItem Source code is as follows:  DWORD xxxEnableMenuItem (  PMENU pMenu ,  UINT wIDEnableItem ,  UINT wEnable )  {  DWORD dres ;  PMENU pRealMenu ;  PPOPUPMENU ppopup ;  CheckLock (pMenu );  dres = MenuItemState (pMenu , wIDEnableItem , wEnable ,  MFS\_GRAYED, &pRealMenu );  /\*  \* If enabling/disabling a system menu item, redraw the caption buttons  \*/  if (TestMF (pMenu , MFAPPSYSMENU) && (pMenu ->spwndNotify != NULL) && (wEnable != dres )) {  TL tlpwnd ;  switch (wIDEnableItem ) {  case SC\_SIZE:  case SC\_MOVE:  case SC\_MINIMIZE:  case SC\_MAXIMIZE:  case SC\_CLOSE:  case SC\_RESTORE:  ThreadLock (pMenu ->spwndNotify , &tlpwnd );  xxxRedrawTitle (pMenu ->spwndNotify , DC\_BUTTONS);  ThreadUnlock (&tlpwnd );  }  }  /\* 367162: If the menu is already being displayed we need to redraw it \*/  if(pRealMenu && (ppopup = MNGetPopupFromMenu (pRealMenu , NULL))){  xxxMNUpdateShownMenu (ppopup , NULL, MNUS\_DEFAULT);  }  return dres ;  }    After reversing the function xxxEnableMenuItem, the reason for the vulnerability is that only the window object is locked, not the menu object in the window object, resulting in the menu object may be reused after release. The patch adds the processing of one reference count to address the problem.  By constructing one in POC, the level 4 menu shown below    xxxRedrawTitle User layer function (xxxCallHook) is called in the function, releasing MenuC, MenuC, and then, the window name object in the window class WNDClass occupies the menu object released in the vulnerability trigger.    The memory layout is at least three consecutive 0x250-byte HWND objects. The middle one is released to construct a 0x250-byte HWNDClass, and the object occupies the released HWND object.  In the xxxRedrawWindow function, use the tail data of the first HWND object (released and occupied by the HWNDClass object) as the parameter for flag validation. Change the cbwndextra in HWNDClass to get the kernel to write arbitrarily.    The latter HWND object with its menu object and its HWNDClass object serves as a medium for the final read and write primitives.  Through the undisclosed function user32! HMValidateHandle The disclosure of kernel information can accurately judge (calculate the spacing of adjacent objects arranged in order) whether the requested window objects are arranged in the order we expect.    Use of the user32! The GetMenuBarInfo function reads with fake tagMENU constructs and can read 16 bytes at a time.    Using the arbitrary write primitive SetClassLongPtr (), it allows the system to allocate extended memory to the window when the window is created. This piece of memory is exclusive to each window. This mechanism provides a way to store window data. The size of this memory is recorded by the cbWndExtra field and can be read and written through the API (GetWindowLong, GetWindowLongPtr, SetWindowLong, SetWindowLongPtr).  Most of the write operation utilizes the class object of the first window object using offset, and the write operation of the replacement TOKEN depends on the class object of the second window, by modifying the Menu of the second window as the false Menu constructed,  After that, the current process EPROCESS address is leaked by \* (\_\_int64 \*) (\* \* (\_\_int64 \* \*) (\* (\* \_\_int64 \*) (spMenu + 0x50) + 0x10) + 0x220)    After the EPROCESS-> ActiveProcessLinks chain list, find the pid 4 process (System process), copy its Token to the current process, complete the extraction. |
| **Use the description results and screenshots** | PoC repetition results    Blue screen  Raise this vulnerability to SYSTEM permission: |

Vi. Use of monitoring and protection

**6.1 Threat hunting ideas and methods**

Not available

**6.2 Detection and alarm rules and protection strategies on the safety equipment side**

Not available