**Windows CLFS Authority promotion vulnerability**

**(CVE-2023-36900)**

**Deep analysis report**

**Catalogue**

[1. Basic information 1](#_Toc145081700)

[2. Threat assessment 2](#_Toc145081701)

[3. The security status of the affected assets 3](#_Toc145081702)

[4. Disposal advice 3](#_Toc145081703)

[5. The full utilization process 4](#_Toc145081704)

[6. Use of monitoring and protection 7](#_Toc145081705)

1. Basic information

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability name** | Windows CLFS Permission Promotion Vulnerability (CVE-2023-36900) | | |
| **Open time** | 2023-08-09 | **refresh time** | 2023-09-07 |
| **CVE number** | CVE-2023-36900 | **Other numbers** | CNNVD-202308-705 |
| **Threat type** | Code execution | **Technology type** | Integer overflow |
| **Manufacturer Name** | Microsoft | **Product Name** | Windows |
| **Real threat state** | | | |
| **POC state** | **EXP state** | **Use state in the field** | **Technical detail status** |
| **partially disclosed** | unknown | Nd | **publiced** |
| **Vulnerability description** | Windows CLFS There is a permission enhancement vulnerability. Authenticated local attackers can exploit this vulnerability by running a special program. The successful exploitation of this vulnerability can be promoted to SYSTEM permission. | | |
| **Influence version** | Windows 10 for 32-bit Systems  Windows 10 for x64-based Systems  Windows 10 Version 1607 for 32-bit Systems  Windows 10 Version 1607 for x64-based Systems  Windows 10 Version 1809 for 32-bit Systems  Windows 10 Version 1809 for ARM64-based Systems  Windows 10 Version 1809 for x64-based Systems  Windows 10 Version 21H2 for 32-bit Systems  Windows 10 Version 21H2 for ARM64-based Systems  Windows 10 Version 21H2 for x64-based Systems  Windows 10 Version 22H2 for 32-bit Systems  Windows 10 Version 22H2 for ARM64-based Systems  Windows 10 Version 22H2 for x64-based Systems  Windows 11 version 21H2 for ARM64-based Systems  Windows 11 version 21H2 for x64-based Systems  Windows 11 Version 22H2 for ARM64-based Systems  Windows 11 Version 22H2 for x64-based Systems  Windows Server 2008 for 32-bit Systems Service Pack 2  Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)  Windows Server 2008 for x64-based Systems Service Pack 2  Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)  Windows Server 2008 R2 for x64-based Systems Service Pack 1  Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)  windows server 2012  Windows Server 2012 (Server Core installation)  Windows Server 2012 R2  Windows Server 2012 R2 (Server Core installation)  Windows Server 2016  Windows Server 2016 (Server Core installation)  Windows Server 2019  Windows Server 2019 (Server Core installation)  Windows Server 2022  Windows Server 2022 (Server Core installation) | | |
| **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)** | |
| 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 successfully exploiting the vulnerability can increase the permission to an 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 to update to the 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-2023-36900 | |
| **Repair solution (including vulnerability patches)** | Microsoft has now released a security update, and users can obtain it through the Windows update. If it cannot update 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-2023-36900 | |
| **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.  Change those in the blf file:  CLFS\_CONTROL\_RECORD->eExtendState  CLFS\_CONTROL\_RECORD->iExtendBlock  CLFS\_CONTROL\_RECORD->iFlushBlock  CLFS\_CONTROL\_RECORD->cNewBlockSectors  CLFS\_CONTROL\_RECORD->cExtendSectors |
| **Use details to describe** | dependency structure:  typedef struct \_CLFS\_CONTROL\_RECORD  {  CLFS\_METADATA\_RECORD\_HEADER hdrControlRecord ;  ULONGLONG ullMagicValue ;  UCHAR Version;  CLFS\_EXTEND\_STATE eExtendState ;  USHORT iExtendBlock ;  USHORT iFlushBlock ;  ULONG cNewBlockSectors ;  ULONG cExtendStartSectors ;  ULONG cExtendSectors ;  CLFS\_TRUNCATE\_CONTEXT cxTruncate ;  USHORT cBlocks ;  ULONG cReserved ;  CLFS\_METADATA\_BLOCK rgBlocks [ANYSIZE\_ARRAY];  } CLFS\_CONTROL\_RECORD, \*PCLFS\_CONTROL\_RECORD;  CLFS. Of sys, function CClfsBaseFilePersisted:: an integer overflow vulnerability in ExtendMetadataBlockDescriptor. CClfsBaseFilePersisted:: The ExtendMetadataBlockDescriptor function is used to extend the metadata block descriptors. The function functions to add new metadata block descriptors at the end of the metadata block descriptor to extend the size of the metadata block. This function is usually called when the metadata block is full to add more space to the metadata block.  The ExtendMetadataBlockDescriptor function may have an integer overflow if the original metadata block is not aligned to the sector size.    It can be observed at the following locations  bu CLFS!CClfsBaseFilePersisted ::ExtendMetadataBlockDescriptor+0xa0  CLFS!CClfsBaseFilePersisted ::ExtendMetadataBlockDescriptor+0x1e1    The value stored in the r 12 register represents the v 10 seen during the static analysis, after the following calculation, causing an integer overflow  mov r12d, 0 xfe 02-> 0x144 designed in dword ptr [rsp + 0A8h + var\_80] / / poc  dec r12d  add r12d, ecx  neg ecx  and r12d, ecx      The value of r12 is passed down, after the following calculation  mov r8d, 0x202-> 0x128 0x140 designed in dword ptr [ra + r14 \* 8 + 8] / / poc  mov ebx , r12d  sub ebx , r8d  mov r8d, ebx  Pass to r 8, Windows uses the fastcall call convention, the memset function rcx rdx r 8 register passes parameters.memset (Address, 0,0x 00000000fffffdfe) causes overline writing.    And eventually caused to crash the system. |
| **Use the description results and screenshots** | PoC repetition results    Trigger Blue screen |

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