Hive Pro

THREAT ADVISORY

Attackers exploit Windows vulnerability to gain admin privilege

TA2022021

Threat Level RED

Publish Date – Jan 31, 2022

Microsoft fixed a privilege escalation vulnerability , CVE-2022-21882, in their January 2022 patch Tuesday release that impacts Windows 10 and Windows Server 2019 if successfully exploited.

CVE-2022-21882 is a vulnerability that allows an attacker with limited access to a compromised device to get administrative privileges, propagate across the network, create new administrators, and execute privileged commands. This is a workaround for the previously patched and actively exploited flaw CVE-2021-1732, which was fixed a year ago that affects Windows 10, Windows 11, Windows Server 2019, and Windows Server 2022. Full exploits, on the other hand, only affected Windows 10 and Windows Server 2019. A Proof of Concept(PoC) for this vulnerability has recently been released by the researchers due to their frustration on Microsoft's bug bounty program.

The following is the exploitation flow:

1. To exploit the issue and obtain an out-of-bounds write, change the cbWndExtra of the window object to 0x0FFFEFFF, allowing the window object WndExtra to access huge amounts of memory.
2. Change the WS_CHILD flag of another window and assign it a specially generated Menu (fake menu).
3. Using the GetMenuBarInfo API and a false menu, get any arbitrary read primitive.
4. To obtain an arbitrary write primitive, use the SetWindowLongPtrA API to alter the ExtraBytes of another window object.
5. Using EPROCESS ActiveProcessLinks, detect the system eprocess with PID 4.
6. Replace the current process token with the system token.

Organizations should apply the patches as soon as possible to avoid exploitation.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-21882	Windows 10 Versions 1809, 1909, 21H1, 20H2, 21H2, Windows Server Versions 2019, 2022, 20H2, Windows 11	cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_11:*:*:*:*:*:*:*:*	Win32k Elevation of Privilege Vulnerability	CWE-269

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21882

References

https://www.bleepingcomputer.com/news/microsoft/windows-vulnerability-with-new-public-exploits-lets-you-become-admin/
https://nvd.nist.gov/vuln/detail/CVE-2022-21882
https://www.borncity.com/blog/2022/01/31/windows-10-proof-of-concept-fr-schwachstelle-cve-2022-21882/
https://googleprojectzero.github.io/0days-in-the-wild//0day-RCAs/2022/CVE-2022-21882.html