Hive Pro

THREAT ADVISORY

Critical Vulnerabilities revealed in Microsoft's patch Tuesday

TA202129

Threat Level RED

Publish Date – Aug 11, 2021

Multiple vulnerabilities have been patched by Microsoft in the month of Aug 2021 Patch Tuesday. Three of them have been labeled as zero-day vulnerabilities (CVE-2021-36936, CVE-2021-36942, and CVE-2021-36948). One of them (CVE-2021-36948) has already been exploited in the wild. The attacker is yet to be identified. Microsoft has classified six vulnerabilities as critical, and patches for all of them are now available.

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name
CVE-2021-36948	Microsoft Windows 10 20H2,10 21H1,10 1809,10 1909,10 2004, Server 20H2, Server 2004, Server 2019	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Windows Update Medic Service Elevation of Privilege Vulnerability
CVE-2021-34530	Microsoft Windows 10 20H2, 10 21H1, 10 1607,10 1809, 10 1909, 10 2004, Server 20H2, Server 2004, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-34534			Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-36936	Microsoft Windows 8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, RT 8.1, Server 20H2, Server 2004, Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-26432			Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability

Hive Pro

THREAT ADVISORY

CVE ID	Affected Versions	Affected CPE	Vulnerability Description
CVE-2021-34480	Microsoft Windows 7 SP1, 8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, RT 8.1, Server 20H2, Server 2004, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_7:sp1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Scripting Engine Memory Corruption Vulnerability
CVE-2021-34535			Remote Desktop Client Remote Code Execution Vulnerability
CVE-2021-26424			Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-36942	Microsoft Windows Server 20H2, Server 2004, Server 2008 R2 SP1,Server 2008 SP2,Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*	Windows LSA Spoofing Vulnerability (CWE-200)

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36948
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34530
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34534
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36936
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26432
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34480
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34535
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942

References

https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2021-patch-tuesday-fixes-3-zero-days-44-flaws/