Hive Pro

THREAT ADVISORY

Emergency patches have been released by Microsoft for PrintNightmare

TA202122

Threat Level Red

Publish Date – July 8, 2021

Attackers have been targeting Windows Print Spooler services for almost 2 months now. It started with the vulnerability(CVE-2021-1675) being exploited in the wild. Soon a patch was released for the same. It was after 2 days that Microsoft found out that there exist another vulnerability which gives the attacker an access to execute a code in the victim's system. This new vulnerability(CVE-2021-34527) has been named as PrintNightmare. An emergency patch has been released by Microsoft for some of the versions and a workflow as been made available for other versions.

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name	CWE ID
CVE-2021-1675	Microsoft Windows version 7 SP1,8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, RT 8.1, Server 20H2, Server 1909, 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:1909:*:*:*:*:*:*:*, 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 Print Spooler Privilege Elevation Vulnerability	CWE-269
CVE-2021-34527			Windows Print Spooler Remote Code Execution Vulnerability	

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1675
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34527

References

https://securelist.com/quick-look-at-cve-2021-1675-cve-2021-34527-aka-printnightmare/103123/
https://attackerkb.com/topics/MIHLz4sY3s/cve-2021-34527-printnightmare?referrer=notificationEmail#rapid7-analysis
https://www.kaspersky.com/blog/printnightmare-vulnerability/40520/