Hive Pro

THREAT ADVISORY

Weren't you warned about reactivating the Print Spooler?

TA202126

Threat Level Red

Publish Date – July 18, 2021

After almost 10 days of releasing an advisory by the Hive Pro Threat Research team, a new vulnerability has been found in Windows Print Spooler. This is a privilege escalation flaw that allows attackers to run arbitrary code with SYSTEM privileges, giving them the ability to install programs, read, alter, or remove data, and create new accounts with full user rights. The affected versions have not been known as of now. There have been no patches released yet, but workarounds are available.

Vulnerability Details

CVE ID	Affected CPEs	Vulnerability Name
CVE-2021-34481	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Microsoft windows print spooler service Privilege Escalation

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34481

References

https://threatpost.com/microsoft-unpatched-bug-windows-print-spooler/167855/
https://arstechnica.com/gadgets/2021/07/disable-the-windows-print-spooler-to-prevent-hacks-microsoft-tells-customers/