AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Windows Print Spooler Remote Code Execution Vulnerability

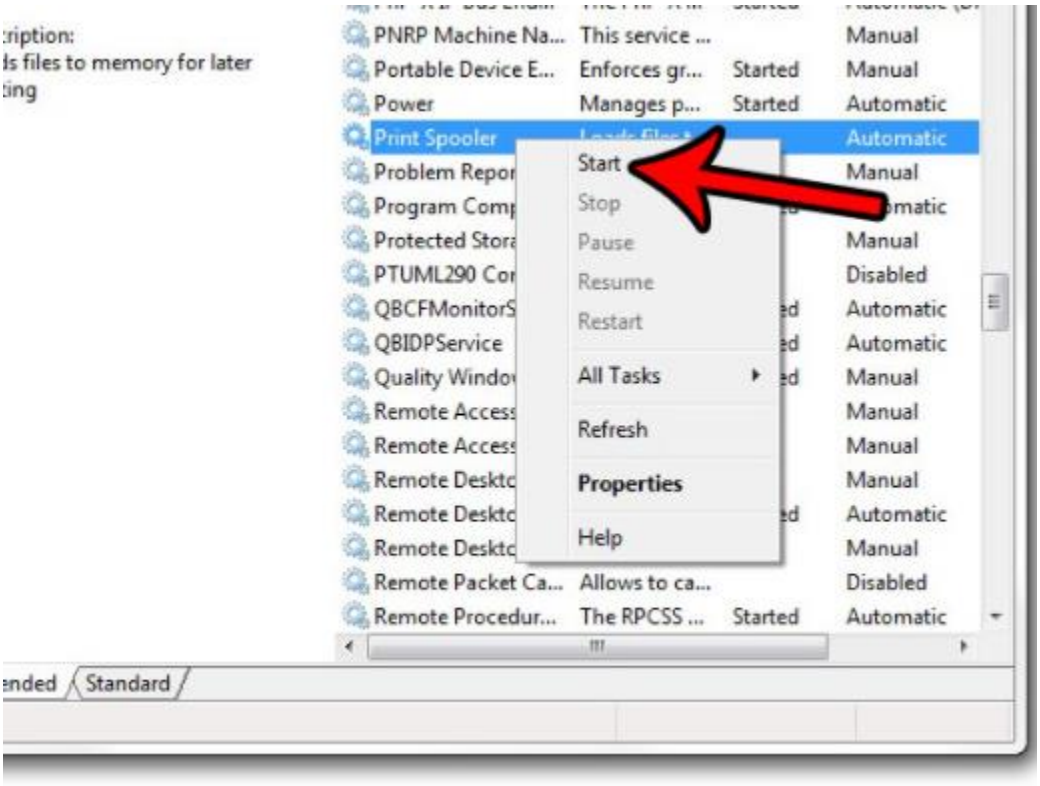
(CVE-2021-34527)

05/07/2021

Autoriteti Kombëtar për Certifikim Eletronik dhe Sigurinë Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Përmbledhje CVE-2021-34527



Ky vulnerabilitet (CVE-2021-34527), është konfirmuar nga Microsoft i cili konfirmon praninë e cënueshmërisë së kodit në të gjitha versionet e Windows. Microsoft po paralajmëron për një vulnerabilitet kritik në shërbimin Windows Print Spooler.

Microsoft i ka caktuar CVE-2021-34527[1], dobësisë së ekzekutimit të kodit në distancë të print spooler-it të njohur si “PrintNightmare” dhe konfirmoi që kodi burim, po përgjon në të gjitha versionet e Windowsit.

Microsoft gjithashtu konfirmoi se ky problem ishte i dallueshëm nga CVE-2021-1675[2], e cila kishte të bënte me një vektor tjetër sulmi dhe një cenueshmëri të ndryshme në RpcAddPrinterDriverEx (). Azhurnimi i Sigurisë i Qershorit 2021 merrej me të, sipas Microsoft, dhe nuk paraqiti probleme të mëtejshme. Kjo kishte ekzistuar para azhurnimit.

"PrintNightmare" është emëruar mirë, pasi lejon një sulmues të ekzekutojë një kod arbitrar me privilegjet e SYSTEM. Kjo dobësi u zbulua në fillim të javës së parë të muajit korrik 2021 pasi studiuesit e sigurisë publikuan aksisdentalisht një shfrytëzim të provës së konceptit (PoC).[3] Ndërsa Microsoft nuk e ka vlerësuar dobësinë, vulnerabiliteti lejon sulmuesit të ekzekutojnë në distancë kodin me privilegje të nivelit të sistemit, i cili është po aq kritik dhe problematik sa mund të merrni akses të plotë në Windows.
Studiuesit në Sangfor publikuan PoC, në atë që duket se ka qenë një gabim, ose një komunikim i gabuar midis studiuesve dhe Microsoft. Kodi i testit u fshi shpejt, por jo para se ai të ishte hedhur tashmë në GitHub. Studiuesit e Sangfor kishin planifikuar të detajonin dobësitë e shumta 0-Days në shërbimin Windows Print Spooler në konferencën vjetore të sigurisë Black Hat më vonë këtë muaj (Korrik 2021). Duket se studiuesit menduan se Microsoft e kishte rregulluar këtë dobësi të veçantë, pasi kompania publikoi rregullime për një të metë të veçantë të Windows Print Spooler.

Siç raportoi *The Reg*, një keqbërës duke shfrytëzuar me sukses dobësinë (përmes një defekti në shërbimin Windows Printer Spooler) mund të instalojë programe, të luajë me të dhëna, ose të krijojë llogari të reja me të drejtat e përdoruesit të plotë.

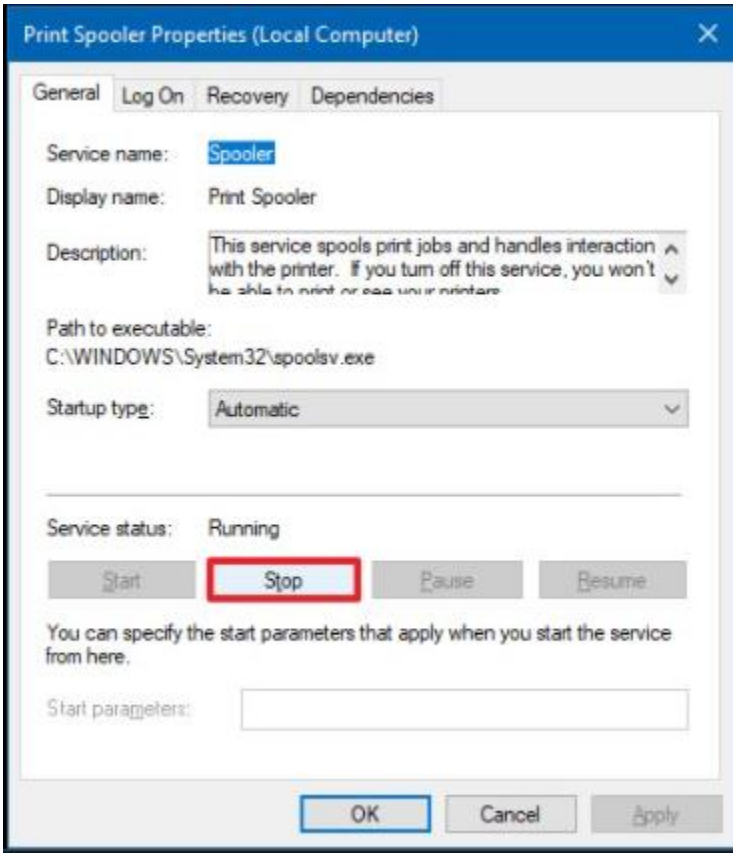
[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1675

[3] https://twitter.com/edwardzpeng/status/1409810304091889669

Microsoft konstatoi se: një sulm, "duhet të përfshijë një përdorues të autentifikuar duke thirrur RpcAddPrinterDriverEx ()."

Microsoft-it i janë dashur disa ditë për të lëshuar më në fund një alarm në lidhje me 0-days. Microsoft po punon për nxjerrjen e një azhurnimi, por derisa të jetë në dispozicion kompania rekomandon çaktivizimin e shërbimit Windows Print Spooler (nëse kjo është një mundësi për bizneset), ose çaktivizimi i printimit përbrenda përmes politikave të Grupit.



Agjencia e Sigurisë Kibernetike dhe e Sigurisë së Infrastrukturës (CISA) ka rekomanduar [4]që administratorët "të çaktivizojnë shërbimin Windows Print Spooler në Domain Controllers dhe sistemet që nuk printojnë".

[4] https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

PrintNightmare, Critical Windows Print Spooler Vulnerability

Original release date: June 30, 2021 | Last revised: July 02, 2021

Print Tweet Send Share

(Updated July 2, 2021) For new information and mitigations, see Microsoft's updated guidance for the Print spooler vulnerability (CVE-2021-34527) .

(Updated July 1, 2021) See Microsoft's new guidance for the Print spooler vulnerability (CVE-2021-34527) and apply the necessary workarounds.

(Original post June 30, 2021) The CERT Coordination Center (CERT/CC) has released a VulNote for a critical remote code execution vulnerability in the Windows Print spooler service, noting: "while Microsoft has released an update for CVE-2021-1675 , it is important to realize that this update does not address the public exploits that also identify as CVE-2021-1675." An attacker can exploit this vulnerability—nicknamed PrintNightmare—to take control of an affected system.

CISA encourages administrators to disable the Windows Print spooler service in Domain Controllers and systems that do not print. Additionally, administrators should employ the following best practice from Microsoft's how-to guides , published January 11, 2021: "Due to the possibility for exposure, domain controllers and Active Directory admin systems need to have the Print spooler service disabled. The recommended way to do this is using a Group Policy Object."

Linku për azhurnimet dhe për referencat:

1. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34527
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527
3. https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability
4. https://www.theregister.com/2021/07/02/printnightmare_cve/
5. https://www.theregister.com/2021/07/01/printnightmare_windows_fix/
6. https://www.theregister.com/2021/06/30/windows_print_spool_vuln_rce/