HC3: Cybersecurity Vulnerability Bulletin

July 06, 2021 TLP: White Report: 202107061000

PrintNightmare, Windows Print Spooler Remote Code Execution Vulnerability

Executive Summary

PrintNightmare is the name given to a critical remote code execution vulnerability in the Windows Print spooler service. Attackers can take advantage of this vulnerability to gain control of affected systems.

The Cybersecurity and Infrastructure Security Agency (CISA) advises all organizations to follow Microsoft's guidance for CVE-2021-34527 and implementing Microsoft's best practice from January 11, 2021. Additional background information can be found in the document published by the CERT Coordination Center.

CISA and Microsoft are continually updating information relating to this vulnerability.

Importance to HPH Sector

This vulnerability affects organizations both within and without the HPH Sector and has the potential to cause widespread harm.

Recently Published Information

CISA
PrintNightmare, Critical Windows Print Spooler Vulnerability
https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

Microsoft
CVE-2021-34527 - Windows Print Spooler Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Microsoft
Security assessment: Domain controllers with Print spooler service available
https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-print-spooler

CERT Coordination Center
Microsoft Windows Print Spooler RpcAddPrinterDriverEx() function allows for RCE
https://www.kb.cert.org/vuls/id/383432

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback