HC3: Alert

July 15, 2021 TLP: White Report: 202107151300

PrintNightmare, Windows Print Spooler Service Vulnerability (Update 1)

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.

Cybersecurity and Infrastructure Security Agency (CISA) advises all organizations follow Microsoft's guidance for CVE-2021-34527 and also implement Microsoft's best practice from January 11, 2021.

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

Report

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

Impact to HPH Sector

This vulnerability affects organizations both within and without the HPH Sector and has the potential to cause widespread harm. Please remain informed on updates to this vulnerability as new information is reported.

References

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 (best practice)
https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-print-spooler

CISA - Emergency Directive 21-04 - Mitigate Windows Print Spooler Service Vulnerability
https://cyber.dhs.gov/ed/21-04/

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