Web Version

From the Division of Critical Infrastructure Protection | Office of Security, Intelligence, and Information Management

ASPR
ASSISTANT SECRETARY FOR
PREPAREDNESS AND RESPONSE

Healthcare and Public Health Sector Cybersecurity Notification

Cyber Response Call on Mitigation Steps for the Critical Microsoft Windows PrintNightmare Vulnerability

This email notification was produced by the Division of Critical Infrastructure Protection (CIP) within the U.S. Department of Health and Human Services' (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR).

Call Details

HHS ASPR and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) are hosting a call on mitigtaion steps for the critical Microsoft PrintNightmare vulnerability from **1:00 - 3:00 PM ET on Thursday, July 22**. The PrintNightmare vulnerability is a “critical” exploit that affects the Windows print queue. This vulnerability allows attackers to execute remote code on your devices and take control of them. The mitigation process for the PrintNightmare vulnerability is a complicated and multistep process. Applying the patch is the first step, but there are more steps required. Please join the call and review the materials in the resources section for remediation steps necessary beyond the patch.

Call Details

Time: 1:00 - 3:00 PM ET on Thursday, July 22
Participant Dial-in: 800-857-6546
Participant Pin: 6326958

Subject matter experts (SME) will provide an explanation of the current alerts on the PrintNightmare vulnerability and the further threat of ransomware it presents. SME’s will also discuss the detail behind mitigations due to their complexity by sharing their lessons/observations from their engagements with Federal entities also dealing with this vulnerability.

The intent of this call is to have a technical discussion that is geared more towards security and IT teams, not necessarily the C-suite/Executive/CIO/CISO level. Participants will walk away more confident in their current actions or better prepared to implement the mitigations correctly.

CISA is aware of active exploitation, by multiple threat actors, of the PrintNightmare vulnerability. Exploitation of the vulnerability allows an attacker to remotely execute code with system level privileges enabling a threat actor to quickly compromise the entire identity infrastructure of a targeted organization.

Resources for HPH Stakeholders

- CVE-2021-34527: Windows Print Spooler Remote Code Execution Vulnerability
- CISA PrintNightmare, Critical Windows Print Spooler Vulnerability webpage
- The Department of Homeland Security (DHS) Emergency Directive (ED) 21-04: Mitigate Windows Print Spooler Service Vulnerability. Although ED 21-04 only applies to Executive Branch departments and agencies it is strongly recommends that state and local governments, private sector organizations, and others review ED 21-04 for additional mitigation recommendations.
- Microsoft's July 2021 Security Update Summary and Deployment Information

Subscribe to HPH Sector Cyber Notifications

Did a colleague forward you this HPH Sector Cyber Notification? Receive these cyber notifications directly by subscribing to the HPH Sector bulletins. HPH Sector bulletins inform stakeholders about the most significant issues facing the sector including cybersecurity, medical supply chains, COVID-19, and more. If you are interested in receiving cyber notifications or other HPH Sector bulletins, visit the CIP bulletins subscription webpage.

Comments and Questions

If you have comments or questions, send an email to CIP@hhs.gov. The CIP team will work to answer your inquiries or connect you to the proper entity.

Traffic Light Protocol (TLP) Designation: WHITE

○○○

TLP: WHITE information may be distributed without restriction.

. Disclaimer: ASPR provides the above sources of information for the convenience of the HPH Sector community and is not responsible for the availability or content of the information or tools provided, nor does ASPR endorse, warrant or guarantee the products, services or information described or offered. It is the responsibility of the user to determine the usefulness and applicability of the information provided.

U.S. Department of Health & Human Services, *Office of the Assistant Secretary for Preparedness & Response*
200 C Street, SW
Washington, DC 20024