American Hospital Association
Advancing Health in America

Cybersecurity Advisory

July 7, 2021

Microsoft Releases Security Updates for 'PrintNightmare' Cybersecurity Vulnerability

Cybersecurity & Infrastructure Security Agency encourages users to review Microsoft updates and apply them

Microsoft has released out-of-band security updates to address a remote code execution (RCE) vulnerability — known as PrintNightmare (CVE-2021-34527) — in the Windows Print spooler service. The Computer Emergency Response Team Coordination Center (CERT/CC), part of the Software Engineering Institute at Carnegie Mellon University, last week reported a critical RCE vulnerability impacting the Windows Print Spooler service that allows a remote authenticated attacker to execute arbitrary code with system privileges on a vulnerable system.

The updates are cumulative and contain all previous fixes, as well as protections for CVE-2021-1675. The updates do not include Windows 10 version 1607, Windows Server 2012 or Windows Server 2016 — Microsoft states updates for these versions are forthcoming. According to CERT/CC, "the Microsoft update for CVE-2021-34527 only appears to address the Remote Code Execution (RCE via SMB and RPC) variants of the PrintNightmare, and not the Local Privilege Escalation (LPE) variant." See CERT/CC Vulnerability Note VU #383432 for workarounds for the LPE variant.

The Cybersecurity & Infrastructure Security Agency (CISA) encourages users and administrators to review the Microsoft security updates as well as CERT/CC Vulnerability Note VU #383432 and apply the necessary updates or workarounds. For additional background, see CISA's initial communication.

What You Can Do

Hospital and health system leaders are encouraged to ensure that their information technology, information security and clinical engineering teams are aware of the above information and are taking appropriate recommended action.

Further Questions

For more information on these or other related issues, contact John Riggi, AHA's senior advisor for cybersecurity and risk advisory services, at jriggi@aha.org.