Microsoft warns of PrintNightmare vulnerability due to flaw in Windows Print Spooler

July 5 2021, by Bob Yirka

Credit: Pixabay/CC0 Public Domain

Microsoft and multiple other entities are warning users and entity operators of a vulnerability in Windows Print Spooler that can allow criminals to hack into Windows computers and remotely execute code.

In its post on the company's Security Update Guide, Microsoft labels the vulnerability as CVE-2021-34527, noting that it is aware of the vulnerability and is working on a patch.

The vulnerability known in security circles as PrintNightmare impacts the Windows Print Spooler—a program that handles printing on Windows computers. The Print Spooler achieved a bit of notoriety a decade ago when it was used by a still unnamed entity to destroy nuclear centrifuges being used by Iran to process nuclear fuel. In this new event, security researchers uncovered the vulnerability and unwittingly made it public before Microsoft could send out a patch. They claimed to have believed that Microsoft had already fixed the problem.

The flaw in Print Spooler involves two vulnerabilities. The first is local privilege escalation, which means that a nefarious character accessing a compromised computer with only a low degree of privilege can give themselves admin or system level rights to the machine. The second allows for remote code execution, which can very obviously be weaponized by criminals—it allows for both local access and lateral movement into other systems such as a domain controller.

The vulnerability is described as zero-day, because it gives computer operators no opportunity for detection and thus no time to respond. The mix-up in making the vulnerability public by security firm Sangfor apparently came about due to a prior patch released by Microsoft to fix a related vulnerability in Print Spooler. The company had planned to document the vulnerability at this year's Black Hat conference and thus had made its findings public for attendees. In its warning, Microsoft noted that users are currently being exploited.

It is not clear when Microsoft will issue a patch, but they suggest users, or more likely IT administrators, disable the Print Spooler until the patch is issued. Users or managers also have the option of disabling remote printing via the Group Policy option.

Citation: Microsoft warns of PrintNightmare vulnerability due to flaw in Windows Print Spooler (2021, July 5) retrieved 3 May 2024 from https://techxplore.com/news/2021-07-microsoft-printnightmare-vulnerability-due-flaw.html