THREAT BULLETINS

PrintNightmare - Microsoft Windows Print Spooler Remote Code Execution Vulnerability

TLP:WHITE

Jul 01, 2021

On June 30, 2021, the CERT Coordination Center (CERT/CC) released a Vulnerability Note (VU#383432) related to **PrintNightmare**, a critical remote code execution (RCE) vulnerability impacting the Windows Print Spooler service. The flaw allows a remote authenticated attacker to execute arbitrary code with SYSTEM privileges on a vulnerable system due to the Microsoft Windows Print Spooler service failing to restrict access to a native functionality.

PrintNightmare was inadvertently disclosed prematurely in connection with CVE-2021-1675 which also affects the Print Spooler service.

Patching of the **PrintNightmare** vulnerability within Microsoft Windows Print Spooler service should be prioritized within your environment pending a determination of the effectiveness of the available patch.

The patch, according to many, appears to fail against the RCE aspect of the vulnerability. One researcher on Twitter shared insight that the **Microsoft Patch works effectively** provided administrators remove “Authenticated users” from “Builtin\Pre-Windows 2000 Compatible Access.”

The recent disclosure of an RCE Proof-of-Concept for PrintNightmare was done so in confusion over another Print Spooler vulnerability. Researchers at Sangfor assumed that their RCE Proof-of-Concept affecting Windows Print Spooler was the same as CVE-2021-1675 which had already been patched. The Proof-of-Concept exploit code which exploits the RpcAddPrinterDriverEx() function was shared on Github prior to its removal upon realizing the mistake.

The RpcAddPrinterDriverEx() function is used to install a printer driver on a system. One of the parameters to this function is the DRIVER_CONTAINER object, which contains information about which driver is to be used by the added printer. The other argument, dwFileCopyFlags, specifies how replacement printer driver files are to be copied. Although authentication is needed first, once an attacker obtains credentials, they can take advantage of the fact that any authenticated user can call RpcAddPrinterDriverEx() and specify a driver file that lives on a remote server. This results in the Print Spooler service spoolsv.exe executing code in an arbitrary DLL file with SYSTEM privileges.

While Microsoft has released an update for CVE-2021-1675, it is important to realize that this update does not address the public exploits that also identify as CVE-2021-1675. Exploit code for this vulnerability that targets Active Directory domain controllers is publicly available on Github.

Reference(s)	cisa, US-CERT, Bleeping Computer, GitHub, GitHub, Microsoft, Twitter, GitHub, Microsoft

Recommendations

- Administrators are encouraged to disable systems that act as print servers.
- Administrators should employ the following best practices from Microsoft’s how-to guide.
- Block port 445/TCP and 135/TCP at your perimeter.

- Enable "PrintService-Operational" event logging in addition to considering Sigma rules for detecting print spooler exploitation.

Sources
CISA: PrintNightmare, Critical Windows Print Spooler Vulnerability

CERT Coordination Center: Microsoft Windows Print Spooler Function Allows for RCE

Public Windows PrintNightmare 0-Day Exploit Allows Domain Takeover

CVE-2021-1675 Print Spooler Exploitation

Detection and Remediation Information for CVE-2021-1675

Windows Print Spooler Remote Code Execution Vulnerability

Alert ID 58b9f3e6

View Alert

Tags PrintNightmare, Microsoft

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.