Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 137 **09-07-2021**

Name: Microsoft Windows Print Spooler RCE Vulnerability (CVE-2021-34527)

Threat Classification: Remote Code Execution

Affected Systems: All editions of Windows where Print Spooler service is enabled

Summary:

The actively exploited security flaw known as '**Print Nightmare'** affects the **Microsoft Windows Print Spooler** service which allows multiple users to access a printer. An attacker who successfully exploits this vulnerability could run arbitrary code with SYSTEM privileges and then can install programs; view, change, or delete data; or create new accounts with full user rights.

Severity	**Critical**
Attack Vector	**Network**
Privileges required	**Low**

For further details, please visit following official link:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Recommendations:

- Please visit the following link for the remediation of the aforementioned vulnerabilities:

  https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7

- It is highly recommended to immediately install the latest Windows updates released on or after **July 6, 2021** on all supported Windows client and server operating systems, starting with devices that currently host the print spooler service.
- User may see the FAQ and Workaround sections of the above-mentioned link for information on how to help protect your system from this vulnerability.
- Always use licensed Antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security/ Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.