GOVERNMENT OF PAKISTAN
CABINET DIVISION, CABINET SECRETARIAT
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)
*****

No. 1-5/2003(NTISB-II) Islamabad 15 July, 2021

Subject:- **Advisory - Windows Print Spooler Remote Code Execution Vulnerability (Advisory No. 46)**

On **6** July 2021, Microsoft has announced on its official Twitter account **(@MsftSecIntl)** and website **(msrc.microsoft.com)** that a critical vulnerability in Windows Print Spooler Service is allowing attackers to gain **system-level privileges** and allows **remote code execution.** These flaws **(CVE-2021-34527** and **CVE-2021-1675)** affect all Windows versions and are being actively exploited. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned to apply Microsoft latest updates and disable Windows Print Spooler Service till the patch is released by the Microsoft.

2. Forwarded for information and dissemination to all concerned, please.

19 JUL 2021
M (Admin | HR)
A.S (Rev. Div.)
M (I.T)
27 JUL 2021
C(A&F) S(Coord)

Major
(Ch Usman Firdous)
Assistant Secretary - II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to:-

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Secretary, NTISB, Cabinet Division, Islamabad
7. Deputy Secretary, NTISB, Cabinet Division, Islamabad
8. Director (IT), Cabinet Division, Islamabad

105058-R
FBR eDOX Dy.No.....
Received in Chairman's Secttt
on 19 JUL 2021

Annexure-A

Subject:- **Advisory - Windows Print Spooler Remote Code Execution Vulnerability (Advisory No. 46)**

1. **Context.** On 6 July 2021, Microsoft has announced on its official Twitter account **(@MsftSecIntl)** and website **(msrc.microsoft.com)** that a critical vulnerability in Windows Print Spooler Service is allowing attackers to gain system-**level privileges** and allows **remote code execution.** These flaws **(CVE-2021-34527** and **CVE-2021-1675)** affect all Windows versions and are being actively exploited. Therefore, mitigation techniques mentioned at **Para 5** must be followed till the patch is released by the Microsoft.

2. **Vulnerabilities Exploited**

   a. **CVE-2021-34527.** Windows Print Spooler Remote Code Execution Vulnerability.

   b. **CVE-2021-1675.** Windows PraAint Spooler Elevation of Privilege Vulnerability.

3. **Vulnerability Impact**

   a. The attacker can remotely control affected systems and run code with system-level privileges.

   b. The attacker can install programs, modify data and create new accounts with admin rights.

   c. The attacker gets full domain administrative permissions with on conclusive traces of exploit in logging files.

   d. The attackers can infiltrate large organizations for data extraction, encryption and infect individual users to expand botnets or launch cryptomining networks.

4. **Windows Versions.** All versions of Windows clients and servers are affected including **Windows 7, 8.1, 10** as well as **Server 2004, 2008, 2012, 2016** and **2019.**

5. **Mitigation Techniques**

   a. **Windows Updates.** Update windows for **CVE-2021-1675** with **June 2021 security updates.** No patches are available for **CVE-2021-34527,** thus, it is important to disable Print Spooler. To see if service is running, type command; **Get-Service -Name Spooler** in Windows cmd.

   b. **How to Disable Print Spooler Service:-** Following steps may be followed:-

      (1) Open Powershell

      (2) Use commands; **Stop-Service-Name Spooler-Force** and then **Set-Service-Name Spooler-StartupType Disabled**

c. **How to Disable Print Spooler Service through Group Policy.**

Disable inbound remote printing through Group Policy by following steps: -

(1) Open Group policy

(2) Go to Computer Configuration / Administrative Templates / Printers

(3) **Disable** "Allow Print Spooler to accept client connections"

d. **Misc Techniques to Disable Print Spooler Service.**

(1) Disable print spooler service via administrative command prompt by typing command **net stop spooler.**

(2) Disable print spooler service via system configurations; click Win key+R,select Services tab and uncheck Print Spooler.

(3) Disable windows print spooler service in domain controllers and systems that do not print.

(4) Block RPC (135 / tcp) and SMB (139 / tcp and 445 / tcp) ports at firewall as a precaution.

6. **Reporting of Suspicious Files/ Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

asntisb2@cabinet.gov.pk

7. Forwarded for perusal and dissemination of information to all concerned and under command, please.