There is a critical vulnerability (**Microsoft Security Bulletin MS17-010**) in various versions of Microsoft Windows (client as well as server) which is being used to spread **ransomware** across the globe.

The **ransomware** is spreading like wild fire infecting critical installations like healthcare globally.

So it is requested to kindly follow the steps listed below to ensure safety of our installations at the earliest.

Following Steps need to be taken to ensure safety of the ICT infrastructure and critical installations of every department:-

1. Ensure that ports TCP/UDP 445 are blocked on all perimeter devices and internal access control devices.

2. Ensure that ports TCP/UDP 445 are blocked on all clients & servers using host firewalls through host anti viruses and HIPS.

Steps for blocking TCP/UDP Port 445 in windows firewall in windows 7 and higher version :-

a. Go to Control Panel and then Windows Firewall

b. Click on Advance Settings

c. Click on Inbound Rules (left Hand Side)and then Action (Top)

d. Click on New Rule (Right hand Side)

e. Select Port and Click Next

f. Select TCP and Select Specific Local Ports and enter 445 and Click Next

g. Select Block the Connection and Click Next.

h. Select Domain, Private & Public and Click Next

i. Give Name Block_TCP_445 (Block_UDP_445 for UDP Port) and Click Finish

j. Repeat the same steps to block UDP Port also

Note: Restart the System to apply the rule effectively.

3. Patch all the Microsoft Windows (client and server) for the vulnerability mentioned in the Microsoft Security Bulletin MS17-010 from link https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

4. Ensure the Antivirus of the clients & server need to be up to date.

5. In case any further Technical Help / Support required regarding this please call at **033 25846233** or mail at **wbbrs@nic.in .**

- National Informatics Centre, North24 Parganas District Centre