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

No. 1-5/2003 (NTISB-II) Islamabad 23 July, 2021

28 JUL 2021

Subject: **Cyber Security Advisory: Windows Server Zero-Day Vulnerability without Patch (Advisory No. 47)**

M(Admin/HR)

M(I.T)

1. A permanent zero-day vulnerability has been found in Windows operating system named as **RemotePotato0**. The identified vulnerability is not being patched by the Microsoft on the pretext that servers must defend themselves against **NTLM relay attacks**. The vulnerability may lead to exploitation and Man-in-the-Middle attacks through escalation of privileges from User to Domain Admin. Therefore, an advisory is attached at **Annexure-A** to sensitize all concerned to harden Windows Servers and adopt precautionary measures.

A.S(Rev Div)

2. Forwarded for dissemination to all concerned, please.

Major
(Imran Nazir)
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. Secretary, Aviation Division, Islamabad
5. Additional Secretary-III, Cabinet Division, Islamabad
6. Director General (Tech), Dte Gen, ISI Islamabad
7. Secretary, NTISB, Cabinet Division, Islamabad
8. Deputy Secretary, NTISB, Cabinet Division, Islamabad
9. Director (IT), Cabinet Division, Islamabad

107457-R

CIO/Chief E-I

S(IT)

S(IT-II)

Annexure -A

Subject:- **Cyber Security Advisory: Windows Server Zero-Day Vulnerability without Patch (Advisory No. 47)**

1. **Background.** A permanent zero-day vulnerability has been found in Windows operating system named as **RemotePotato0.** The identified vulnerability is not being patched by the Microsoft on the pretext that servers must defend themselves against **NTLM relay attacks.** The vulnerability may lead to exploitation and Man-in-the-Middle attacks through escalation of privileges from User to Domain Admin. Therefore, mitigation measures at **Para 4** must be applied against Windows Domain Servers.

2. **Vulnerability Details.** Vulnerability in Windows Remote Procedure Call **(RPC)** protocol makes it possible to trigger authenticated IRPC, Distributed Component Object Model **(DCOM)** call and relay NTLM authentication to other protocols.

3. **Windows affected.** Every Windows system is vulnerable.

4. **Mitigation Techniques.** Following mitigation techniques may be opted / configured by admins at Windows Servers: -

   a. **Use of Secure Shell (SSL).** Prefer SSL everywhere where NTLM is used and configure **Channel Binding Tokens validation** by setting **tokenChecking** to **minimum.**

   b. **Configuration of Server Message Block (SMB).** For SMB server, configure SMB signing by setting **Group Policy to digitally sign server communication.**

   c. **Configuration of Domain Controller.** Set Domain Controller as under:-

      (1) Lightweight Directory Access Protocol (LDAP) server channel binding token requirements Group Policy to a minimum (if supported).

      (2) LDAP server signing requirements Group Policy to require signature (for non-LDAP connections).

   d. **Addition of Yara Rule at Firewall.** Yara Rules **(Appendix-I)** may be added on firewall to detect RemotePotato0.

5. **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

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

Appendix-I

ADDITION OF YARA RULES AT FIREWALL

```
Rule RemotePotato0_privesc {meta:Description = "Detect RemotePotato0 binary"
strings:
        $import1 = "CoGetInstanceFromIStrorage"
        $istorage_clsid = "{00000306-0000-0000-c000-000000000046}" nocase
        wide  ascii
        $meow_header = { 4d 45 4f 57 }
        $clsid1 = "{11111111-2222-3333-4444-555555555555}" nocase wide
        $clsid2 = "{5167B42F-C111-47A1-ACC4-8EABE61B0B54}" nocase wide ascii
        condition:
(uint16(0)  == 0x5a4D) and $import1 and $istorage_clsid and $meow_header  and 1
of ($
```