WN10-CC-000290

WN10-CC-000290

The STIG ID **WN10-CC-000290** addresses the requirement that **Remote Desktop Services (RDS) must be configured with client connection encryption set to "High Level."** This is crucial for ensuring that any remote session involving a Windows 10 machine is protected against unauthorized data interception. Remote sessions without strong encryption are vulnerable to network sniffing, session hijacking, and other security threats.

Description:

Remote Desktop Protocol (RDP) sessions can transmit sensitive information such as login credentials, system commands, and file contents. If these sessions are not properly encrypted, malicious actors can potentially intercept and exploit the data. Enforcing **High Level encryption** ensures that both incoming and outgoing data are secured using robust encryption algorithms, safeguarding the integrity and confidentiality of the remote session.

Vulnerability Discussion:

- The MinEncryptionLevel registry setting controls the minimum level of encryption for RDP client connections.
- If this setting is not configured or is set to a value lower than 3 (High), remote sessions may use weak encryption or none at all.
- Weak encryption exposes systems to man-in-the-middle (MITM) attacks and eavesdropping, especially in enterprise or public network environments.

Manual Check:

To verify whether the RDP encryption level is properly configured, follow these steps:

Registry Check:

1. Open **Registry Editor**:
    - Press Win + R, type regedit, and press Enter.
2. Navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
3. Look for MinEncryptionLevel.
4. Ensure the value is set to 3.

Value Mappings:

- 1 = Low
- 2 = Client Compatible
- 3 = High

- 4 = FIPS Compliant

If the key/value is missing or not set to 3 (High), **this is a finding**.

Fix:
You can remediate this issue through either Group Policy or directly via the Registry.

Fix via Group Policy:
1. Open **Group Policy Editor** (gpedit.msc).
2. Navigate to: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security
3. Find the policy:
- **Set client connection encryption level**
4. Configure the policy:
- Set to **Enabled**
- Choose **High Level** from the drop-down menu.
5. Click **Apply**, then **OK**.
- Run gpupdate /force to apply the policy immediately.

Fix via Registry:
1. Open **Registry Editor** (regedit).
2. Navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
3. If **MinEncryptionLevel** does not exist:
- Right-click in the right pane, select **New > DWORD (32-bit) Value**.
- Name it **MinEncryptionLevel**.
4. Set its value to:
- 3 (Decimal) = High Level
5. Close Registry Editor and restart the computer.

This will ensure that all Remote Desktop sessions initiated on the system use strong encryption, aligning with the **WN10-CC-000290** STIG requirement and enhancing your overall system security posture.