

Implementation of Security Measures in IT

By Rajbir Singh

Vulnerability

Deprecated SSL and TLS version

Impact

Critical

Solution

In Windows, create new registry values of SSL version and set their values to DWORD 0.



SSL

- SSL (Secure Sockets Layer) is a cryptographic protocol designed to secure communication between clients and servers over the internet.
- It provides encryption, authentication, and data integrity, ensuring that sensitive information remains private and protected.



Problem with SSL

- **Weak Encryption:**

Older versions of SSL, such as SSLv2 and SSLv3, suffer from known vulnerabilities and weak encryption algorithms.

- **Certificate Validity:**

SSL certificates have a finite validity period, typically ranging from a few months to a few years. If certificate renewal processes are not managed properly, it can lead to expired certificates, resulting in interrupted or insecure connections.




Solution

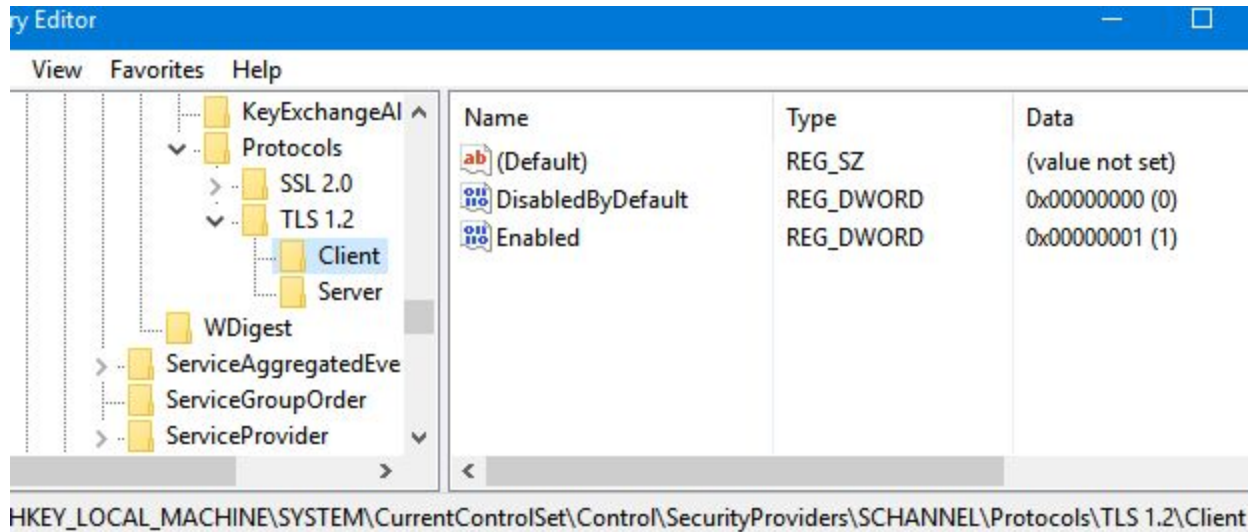
```
reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr  
otocols\SSL 2.0\Client" /v DisabledByDefault /t REG_DWORD /d 1 /f
```

```
reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr  
otocols\SSL 2.0\Client" /v Enabled /t REG_DWORD /d 0 /f
```

```
reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr  
otocols\SSL 2.0\Server" /v DisabledByDefault /t REG_DWORD /d 1 /f
```

```
reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr  
otocols\SSL 2.0\Server" /v Enabled /t REG_DWORD /d 0 /f
```





Vulnerability

SNMP Agent Default Community Name (public)

Impact

High

Solution

Disable SNMP service from printer settings or use SNMP v3.

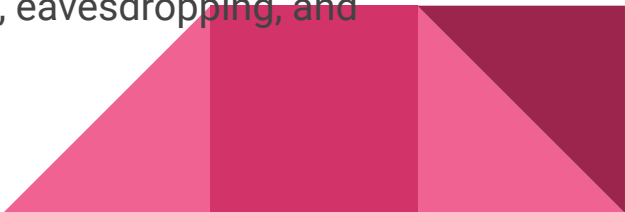


SNMP:

- SNMP (Simple Network Management Protocol) is a widely used network management protocol that enables administrators to monitor and manage network devices and systems.
- It provides a standardized framework for collecting and organizing information about network devices, such as routers, switches, servers, and printers.

Problem:

Security Vulnerabilities: SNMP versions prior to SNMPv3 lack robust security features. SNMPv1 and SNMPv2c use community strings for authentication, which can be easily intercepted and compromised. This makes SNMP communication susceptible to unauthorized access, eavesdropping, and tampering.



Vulnerability

rsh Service Detection

Impact

High

Solution

Disable rsh service from printer settings



rsh (Remote Shell)

RSH (Remote Shell) is a service that allows users to execute commands on remote systems over a network.

This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism.



Vulnerability

Unencrypted Telnet Server

Impact

Medium

Solution

Turn off Telnet from “Turn Windows features on or off” setting in Control Panel



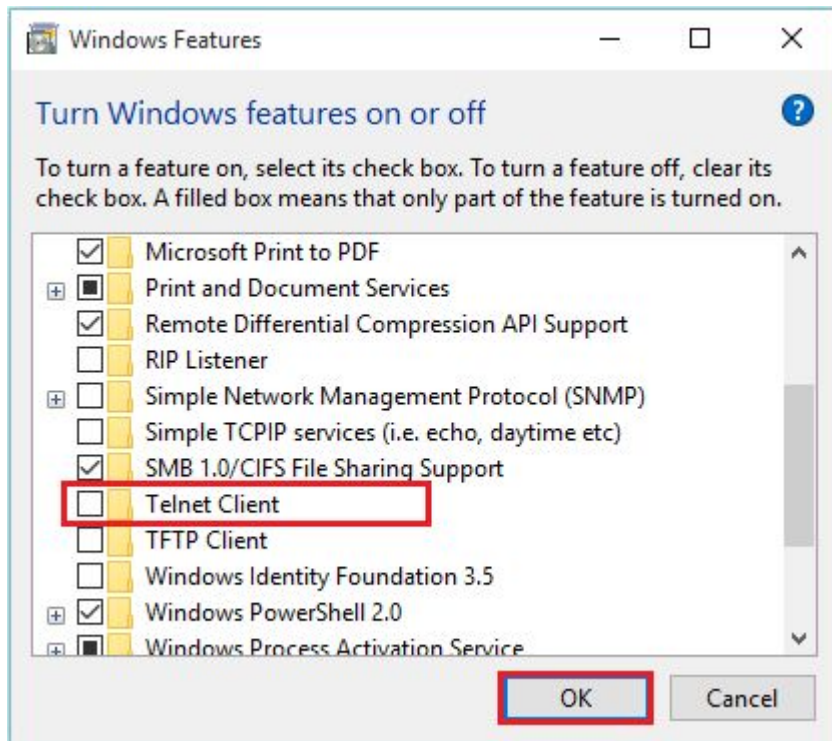
Telnet

- Telnet is a network protocol used for remote access and control of devices over a network.
- It allows a user to establish a text-based, bidirectional communication session with a remote device or server.

Problem with using Telnet:

Telnet transmits data, including usernames, passwords, and commands, in clear text, which makes it vulnerable to eavesdropping and interception.





Vulnerability

SMB Signing not required

Impact

Medium

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.



SMB Signing

- SMB signing, also known as Server Message Block signing, is a security feature in the SMB protocol used by Windows operating systems for file and printer sharing over a network.
- It is designed to ensure the integrity and authenticity of SMB communications between a client and a server. It helps protect against tampering and unauthorized modification of data in transit.



Vulnerability

IP Forwarding Enabled

Impact

Medium

Solution

On Linux, you can disable IP forwarding
by doing :

```
->sudo -i
```

```
->echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters



IP Forwarding

IP forwarding, also known as IP routing, is a fundamental function of network devices, such as routers and switches. It involves the process of forwarding IP packets between different network segments or subnets.

Problem:

An attacker can exploit this to route packets through the host and potentially bypass some firewalls.



More changes to secure a system

- Access Control
- Regular Patching and Updates
- Firewalls
- Monitoring and Auditing
- Encryption



