Technical Report:-

Given below is the technical report for vulnerability Nessus scan on windows 172.31.53.63

Vulnerability	SSL Medium Strength Cipher Suites Supported (SWEET 32)
Reference	CVE 2016 – 2183
Vulnerability Description	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
CVSS 3. Severity and metrics	7.5
NVD Reference	https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info https://nvd.nist.gov/vuln/detail/CVE-2016-2183#vulnCurrentDescriptionTitle
Known Exploit	Unknown
Impact	Data loss via MIMAT(Man in middle Attack). A malicious threat actor can perform MIMT attack on communication channel to exfilter data.
Remediation	Reconfigure the affected application if possible to avoid use of medium strength ciphers. • Disable SSL 3DES Ciphers • Avoid the usage of legacy 64-bit block ciphers • Web servers and VPN should be configured to use 128-bit cipher or above

	• TLS libraries and applications should limit the length of TLS sessions with a 64-bit https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel https://social.technet.microsoft.com/Forums/en-US/2f48865b-ce21-4547-8d7c-6731b0071522/ssl-medium-strength-cipher-suites-vulnerabilities?forum=Exch2016Comp