| **ลำดับที่** | **หมายเลขไอพี** | **รายละเอียดช่องโหว่** | **ระดับความเสี่ยง** | **คำแนะนำในการแก้ไข** |
| --- | --- | --- | --- | --- |
| 1 | 203.150.237.1 203.150.237.2 | SSL Medium Strength Cipher Suites Supported (SWEET32)  - 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. | High | Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
| 2 | 203.150.237.1 203.150.237.2 | TLS Version 1.0 Protocol Detection  - The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | Medium | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. |
| 3 | 203.150.237.12 | SMB Signing not required  - Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | Medium | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. |
| 4 | 203.150.237.12 | PRTG Network Monitor 20.1.57.1745 Information Disclosure (direct check)  - An information disclosure vulnerability exists in PRTG Network Monitor. An unauthenticated, remote attacker can exploit this, via a crafted HTTP request, to disclose information about probes running or the server itself (CPU usage, memory, Windows version, and internal statistics). | Medium | Upgrade to PRTG Network Monitor 20.1.57.1745 or later |