Nessus Vulnerability Scan Report

SSL Medium Strength Cipher Suites Supported (SWEET32)

Plugin ID: 42873
Severity: High
Affected Host: 192.168.29.238:15150 (TCP)

Description:

The server supports SSL cipher suites that use medium strength encryption, specifically the 3DES (Triple DES) algorithm. This makes the server vulnerable to the SWEET32 attack (CVE-2016-2183), which could allow an attacker to recover portions of plaintext from encrypted sessions by analyzing large volumes of captured traffic.

Impact:

An attacker with access to network traffic could exploit SWEET32 by capturing enough encrypted sessions using 3DES-based ciphers, and potentially decrypt sensitive information through statistical analysis.

Solution:

Disable 3DES and other medium-strength ciphers in the server's SSL/TLS configuration. Use strong ciphers such as AES-GCM and restrict protocol versions to TLS 1.2 or TLS 1.3. For example, in Apache you can use: SSLCipherSuite HIGH:!aNULL:!MD5:!3DES SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 Then restart the web server.

References: - https://sweet32.info - https://www.tenable.com/plugins/nessus/42873