TASK-8

Vulnerability Name: TLS Version 1.0 Protocol Detection

CWE:

310: Cryptographic Issues

327: Use of a Broken or Risky Cryptographic Algorithm

OSWAP: A02:2021- Cryptographic Failures

Description:

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.

Business Impact: Security Issues, Compliance Issues, Limited Interoperability.

Affected URL: Chennai.vit.ac.in

Proof of Concept:

Remediation: Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.