Security Vulnerabilities in Azure SQL DB

Last updated by | Subbu Kandhaswamy | Feb 16, 2023 at 1:43 PM PST

Contents

Security Vulnerabilities reported in Azure SQL DB

Symptoms

Customer runs a scan against SQL database using commercial scanner/pentesting tools like Nessus (vulnerability scanner), Tenable or via SSL Labs. The scan report shows multiple vulnerabilities related to older versions of TLS or insecure/weak cipher suites

Cause

SQL Database is a multi-tenant PaaS service with a shared control plane. Hence, we do not have the ability to disable older TLS protocols or weak cipher suites without impacting all our customers.

Mitigations

- Set minimal TLS version to 1.2 on the logical server
- Use the Schannel related registry keys to disable TLS <1.2 and associated ciphers on the client.

For more information, please refer to our Best Practices

Sweet32 attack / removing 3DES

For backward compatibility reasons, 3DES ciphers are currently supported. There are plans to support TLS 1.3 in future, which will remove 3DES.

Response to customer

When you get such cases and if any of the vulnerabilities falls in the above categories, use the above explanations and this should help in deflecting CRI's around these asks.

Classification

Root cause Tree - Security/User issue/error/Vulnerability assessment

Reference

- Sweet32 attack
- Managing SSL/TLS Protocols and Cipher Suites for ADFS

How good have you found this content?