GCN-01323: TLS 1.2 Cipher Changes and Integration Impact (Doc ID 2889538.1)

In this Document

APPLIES TO:

Oracle Taleo Onboarding Cloud Service - Version 22B and later
Oracle Taleo Platform Cloud Service - Passport Framework - Version 22B and later
Oracle Taleo Platform Cloud Service - SmartOrg (Central Configuration) - Version 22B and later
Oracle Taleo Platform Cloud Service - Connect - Version 22B and later
Oracle Taleo Recruiting Cloud Service - Version 22B and later
Information in this document applies to any platform.
TLS 1.2 protocol utilizes cipher suites for the HTTPS connection. This ensures communications between the two parties are encrypted.

DETAILS

GCN-01323, sent on August 10 2022, announces the deprecation of certain TLS 1.2 ciphers (these are used for HTTPS connections).

- August 22th - September 5th, 2022: Deprecated TLS 1.2 ciphers will be removed from TEE and TSS staging zones
- September 6th - September 19th, 2022: Deprecated TLS 1.2 ciphers will be removed from TEE and TSS production zones

Supported (non-deprecated) TLS 1.2 ciphers are listed here:

- *Taleo Application Supported TLS Cipher Suites* (Doc ID 2888935.1) (link)

Note: When an HTTPS connection based on TLS 1.2 is initiated between two parties (client / server), there is a "handshake" that negotiates how the communication between the parties will proceed. During this handshake the most secure cipher suite that is supported by both parties is chosen. (More information about the handshake here (link opens in 3rd party non-Oracle website). After the announced change, deprecated ciphers will not be available for HTTPS connections.

ACTIONS

Impact:

- Any HTTPS connection to the zone after the change must use one of the supported TLS 1.2 ciphers.

Actions:

- TCC: No action needed. Current versions of TCC use Java 1.8 or higher, which already supports the required TLS 1.2 ciphers.

- Web Services API: Custom applications utilizing Taleo web service API must support the required TLS 1.2 ciphers. Customers will have to work with their own IT and developers to determine if any change is needed.
- Passport Services: No action needed. It is thought that passport service providers already support the required TLS 1.2 ciphers. Internal investigation and discussion is in progress.
- TEE Users (not integration): No action needed. Supported browsers already support the required TLS 1.2 ciphers.

REFERENCES

NOTE:2888935.1 - Taleo Application Supported TLS Cipher Suites
NOTE:2455598.1 - TCC: Using Wireshark To Verify TCC Connection's TLS Version
NOTE:1953262.1 - TCC & WebServices API: Unable to Connect or Ping the Zone Due To TLS Handshake Failure
NOTE:2779185.1 - How to Troubleshoot the SSL Connection between TCC and the Zone using the -Djavax.net.debug=all Parameter
NOTE:2155131.1 - Using Wireshark

Didn't find what you are looking for?