ERRMSG: Chrome Browser Warning: "TLS 1.0 or TLS 1.1, which are deprecated and will be disabled in the future."

Users Google Chrome 72 and newer (Feb 2019) may notice a warning message in the browser console

The full message will look something like

[WCS] Warning "The connection used to load resources from https://127.0.0.1:23024 used TLS 1.0 or TLS 1.1, which are deprecated and will be disabled in the future. Once disabled, users will be prevented from loading these resources. The server should enable TLS 1.2 or later. See https://www.chromestatus.com/feature/5654791610957824 for more information." occurs in the console on Chrome when use HTTPS

According to Chrome development team:

Deprecate TLS 1.0 and 1.1, targeting removal in Chrome 81 (early 2020). During the deprecation period, sites using those protocols will show a warning in DevTools. After the deprecation period, in 2020, they will fail to connect if they have not upgraded to TLS 1.2 by then.

Root Cause Analysis

Initially, Atalasoft engineering was looking to make a change/fix to the web capture service itself. However, further investigation has found that the issue is entirely OS configuration related.

After configuration testing we found that only the following OSs need to be updated (enable TLS 1.1 and 1.2):

- Windows Server 2008 R2
- Windows 7

Issue is not reproduced on the following Oss, this means that these systems don't need to be updated:

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

ERRMSG: Chrome Browser Warning: "TLS 1.0 or TLS 1.1, which are deprecated and will be disabled in the future."

- Windows 8.1
- Windows 10

There is no bug in product. WCS uses cpprestsdk as a web-server component, and this server is based on standard WinHttp component, which can be configured to use different protocols. Thus, to enable TLS 1.2 the WinHttp needs to be configured using registry keys.

Fix

By default Windows 7 and Windows Server 2008 R2 support only TLS 1.0, to enable TLS 1.1 and 1.2 following steps should be completed:

1. KB3140245 must be installed on a system;
2. Once this is done, the following Registry keys should be updated

- Add DefaultSecureProtocols DWORD entry with value a00 in the following path

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
- For x64 systems, the path

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp

  should be also updated
- For TLS 1.1 support DisabledByDefault DWORD entry with value 0 should be added to the following paths:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
- For TLS 1.2 support DisabledByDefault DWORD entry with value 0 should be added to the following paths:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

ERRMSG: Chrome Browser Warning: "TLS 1.0 or TLS 1.1, which are deprecated and will be disabled in the future."

External Links / References

- Default protocols support (search for WINHTTP_OPTION_SECURE_PROTOCOLS)
- Microsoft KB3140245
- Configure registry to support newer TLS versions

Original Article:

Q10486 - ERRMSG: Chrome Browser Warning: "TLS 1.0 or TLS 1.1, which are deprecated and will be disabled in the future."

Atalasoft Knowledge Base
https://www.atalasoft.com/kb2/KB/50018/ERRMSG-Chrome-Browser-Warning-TLS-10...