感謝 貴公司對臺灣網路認證公司 TWCASSL 憑證服務的支持。

提醒您:各大瀏覽器廠商將於 2020 年 3 月份起,停止對 TLS 1.0 與 TLS 1.1 傳輸協定之支援。

參考資料

[Safari] https://webkit.org/blog/8462/deprecation-of-legacy-tls-1-0-and-1-1-versions/ [Firefox] https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/ [Edge] https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edge-ie11/ [Chrome] https://security.googleblog.com/2018/10/modernizing-transport-security.html

▶ 現況

Google Chrome 瀏覽器自版本 79 起(2019/12 推出) 已針對網站系統所提供之 TLS 傳輸協定版本進行檢查·若網站無支援 TLS 1.2 傳輸協定即會出現警告訊息(圖一)·Mozilla Firefox 瀏覽器亦有類似安排(圖二)。

過見硆小方戎以女孙(迴二)。



(圖一、Chrome 79, 網站不支援 TLS v1.2 傳輸協定)

▶ 即將實施

目前已知 Google Chrome 瀏覽器將於版本 81 (2020/03 推出)、Mozilla Firefox 瀏覽器將於版本 74 (2020/03 推出) 完全停止對 TLS 1.0 與 1.1 傳輸協定之支援 · 屆時 貴公司網站若無支援 TLS 1.2 傳輸協定,則使用最新瀏覽器之使用者將無法以 HTTPS 方式連線瀏覽 貴公司網站,造成網站使用上之巨大衝擊。 可利用 Qualys SSL Labs 提供之網站 SSL 檢查免費服務,

確認 貴公司網站有無支援 TLS 1.2 傳輸協定:

- 1、 連至以下網址 https://www.ssllabs.com/ssltest/
- 2、 於 Hostname 欄位輸入網址,以本公司網站為例,輸入 www.twca.com.tw,

輸入後請按 "Submit" 開始檢查。

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.

Submit

3、 請稍等片刻, 直到 "Grade" 出現英文字, 代表檢查完成, 再點選 "Server" 欄位

顯示之 IP · 產生結果報告。

	Server	Test time	Grade
1	2001:b031:1306:ff00:0:0:0:1011 2001-b031-1306-ff00-0000-0000-1011.hinet-ip6.hinet.net Ready	Wed, 19 Feb 2020 12:59:38 UTC Duration: 120.8 sec	Α

4、 確認結果報告中 Protocols 章節之 "TLS 1.2" 檢查項目,

Confi	guration	
R	Protocols	No
	TLS 1.2	Yes
	TLS 1.1	No
	TLS 1.0	No
	SSL 3	No
	SSL 2	No
	For TLS 1.3 tests, we only support RFC 8446.	

若檢查結果為"Yes",即代表貴公司網站已支援 TLS 1.2,將不受 3 月份瀏覽器更版之影響;

若檢查結果為"No",即代表貴公司網站尚未支援 TLS 1.2,請盡快安排網站之設定調整作業。

以下針對市面上三種常用的網頁伺服器(IIS、Apache、Tomcat),說明如何設定支援 TLS 1.2 的操作步驟。

- 1 · IIS
 - 1.1 開啟登入編輯程式

於桌面左下角按滑鼠右鍵,點選"執行",於搜尋對話方塊中輸入 regedit 後按"確定" ,開啟「登入編輯程式」。

	N 분위 듣기 : •	
鼎啟(O): reg	gedit	~

1.2 依序展開登入機碼

依序展開 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ SecurityProviders\SCHANNEL\Protocols



1.3 新增 TLS 1.2 機碼

※ 如系統本身已有 TLS 1.2 機碼則無需執行,反之若無,請參照以下步驟新增。 1.3.1 於 Protocols 按右鍵選擇新增,資料類型為機碼。



1.3.2 將新增之新機碼#1 重新命名成 TLS 1.2。



1.3.3 於 TLS 1.2 按右鍵選擇新增,資料類型為機碼。

SasIProfiles SCHANNEL Ciphers Hashes KeyExchangeAlgorithms V - Protocols V - 新機碼 #1	~	名編 	類型 REG_SZ	資料 (數值未設定)	
	>	<			



1.3.6 將新增之新機碼#1 重新命名成 Server。

Ciphers C	s jeAlgorithms t	▲ 名稱 ▲ (預設值)	類型 REG_SZ	資料 (數值未設定)	
<	>	<			>

1.4 修改 TLS 1.2 機碼-Client

1.4.1 於 TLS 1.2 的 Client 按右鍵選擇新增,資料類型為 DWORD(32-位元)值。



	SCHARTEE		「合併	親望	真不计
	Ciphers		•••)(預設值)	REG_SZ	(數值未設定)
			🕮 DisabledByDefault	REG_DWORD	0x00000000 (0)
	KeyExchangeAlgorithms				
~	Protocols				
	✓ - TLS 1.2				
	Server	~	1		
		>	<		

1.4.3 於 DisabledByDefault 按右鍵選擇修改, ·數值設定為 0·按確定 將底數為十六進位 之數值資料 📑 登錄編輯程式 × 檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H) SCHANNEL ~ 名稱 麵型 資料 Ciphers ab (預設值) REG_SZ (數值未設定) CipherSuites 跪 DisabledByDefault 0~0000000 (0) Hashes 修改(M)... KeyExchangeAlgorithms 修改二進位資料(B)... Protocols TLS 1.2 刪除(D) Client 重新命名(R) Server < 電腦\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

數值名稱(N):					
DisabledByDefault					
數值資料(V):	十六進位(H) 十進位(D)				
	確定	取消			
登錄編輯程式	2011 1911 1911			- 0	×
■ 登錄編輯程式 檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 目 ↓ - SCHANNEL	說明(H)	名稱	類型	- □	×
■ 登錄編輯程式 檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 目 ▼ - SCHANNEL Ciphers	說明(H)	名稱 •••) (預設值)	類型 REG_SZ	─ □ 資料 (數值未設定)	×
	說明(H)	名稱 ● (得設値) 部 DisabledByDefault	類型 REG_SZ REG_DWORD	- □ 資料 (數值未設定) 0×00000000 (0)	×

1.5 修改 TLS 1.2 機碼-Server

🎬 登錄編輯程式						×					
福寨(F) 編輯(E) 檢視(V) ✓ SCHANNEL ✓ Giphers CipherSuite Hashes ✓ Keyfxchang ✓ TLS 1.2 CipherSuite	我的最愛(A) 說明(H) s yeAlgorithms	▲ 名稱 ▲ (預設值)	頻型 REG_SZ	資料 (數值未設定)							
<	展開					>					
ŧ碼(K)	新増(N)	trol\SecurityPro	viders\SCHANNEL\Protoc	cols\TLS 1.2\Server	2	54					
字串值(S)	尋找(F)	and the second	/ ///								
- 谁位值(B)											
	Ind Mark (CP)	the second se				重新命名(R)					
	重新命名(R)										
—————————————————————————————————————	重新命名(R) 歴出(F)		/////								
2000RD (32-位元) 值(D) 2000RD (64 位元) 值(Q) 8字串值(M)	重新命名(R) 運出(E) 使用權限(P)										
2000 (32-位元) 值(D) QWORD (64 位元) 值(Q) 多字串值(M) 可擴充字串值(E)	重新命名(R) 重出(E) 使用權限(P) 複製機碼名稱(C)										
2010年11月1日 DWORD (32-位元) 値(D) QWORD (64 位元) 値(Q) 多字串値(M) 可損充字串値(E) 登録編輯程式	重新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C)					×					
2000RD (32-位元) 値(D) 2000RD (64 位元) 値(Q) 多字串値(M) 可擴充字串値(E) 登錄編輯程式 ((F) 編輯(E) 檢視(V) 我的語	重新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	212	1871	-		×					
WORD (32-位元) 值(D) WORD (64 位元) 值(Q) 序串值(M) 博克字串值(E) 登錄編輯程式 (F) 編輯(E) 檢視(V) 我的詞 ✓	重新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稿 (ab)(福职性)	類型 BEG S7			×					
WWORD (32-位元) 値(D) WWORD (64 位元) 値(Q) 5字串値(M) J擴充字串値(E) 登録編輯程式 (F) 編輯(E) 檢視(V) 我的 SCHANNEL Ciphers CipherSuites	重新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稱 (預設值) (期新軟值 #1	類型 REG_SZ REG DWORD	一 資料 (創值未設定) 0x0000000 (0		×					
WORD (32-位元) 値(D) WORD (64 位元) 値(Q) 浮車値(M) 博克字車値(E) 登録編輯程式 (F) 編輯(E) 檢視(V) 我的的 SCHANNEL 	重新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稱 •••) (預設值) [關新數值 #1	頑型 REG_SZ REG_DWORD	 資料 (數值未設定) 0×00000000 (0		×					
WVORD (32-位元) 値(D) WVORD (64 位元) 値(Q) 5字串値(M) 丁増充字串値(E) 登録編輯程式 (F) 編輯(E) 檢視(V) 我的望 ・	utanical 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稱 •••) (預設值) [關新數值 #1	頑型 REG_SZ REG_DWORD	 資料 (數值未設定) 0×00000000 (0		×					
WVORD (32-位元) 値(D) WVORD (64 位元) 値(Q) 5字串値(M) 丁増充字串値(E) 登録編輯程式 (F) 編輯(E) 檢視(V) 我的詞 ・	■ 新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稱 •••) (預設值) [調新數值#1	積型 REG_SZ REG_DWORD	- 資料 (數值未設定) 0×00000000 (0		×					
WWORD (32-位元) 値(D) WWORD (64 位元) 値(Q) 5字串値(M)] 摘充字串値(E) 登録編輯程式 (F) 編輯(E) 檢視(V) 我的望 	■ 新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稱 •••) (預設值) [關新數值 #1	類型 REG_SZ REG_DWORD	 資料 (數值未設定) 0×00000000 (0		×					
2000 (32-位元) 値(D) 2000 (64 位元) 値(Q) 5字串値(M) 可擴充字串値(E) 登録編輯程式 (F) 編輯(E) 檢視(V) 我的語 ○	■ 新命名(R) 重新命名(R) 運出(E) 使用權限(P) 複製機碼名稱(C) 最愛(A) 説明(H)	名稱 •••) (預設值) [關新數值 #1	類型 REG_SZ REG_DWORD	 資料 (數值未設定) 0×00000000 (0		×					

1.5.2 將新增之新數值#1 重新命名成 Enabled。

				- [
案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)		Tetras ora	Terrores	
	^	名稱	類型	資料	
Ciphers		ab) (預設值)	REG_SZ	(數值未設定)	
Hashes		🕫 Enabled	REG_DWORD	0x00000000 (0)	
KevExchangeAlgorithms					
✓ Protocols					
V TLS 1.2					
Client					
Server	~				
	>	<			
≝\HKEY_LOCAL_MACHINE\SYSTEM\CurrentC	ontrolSet\Co	ontrol\SecurityProvid		ls\TLS 1.2\Server	
	ミキキシ レクコ	H			
5.3 於 Enabled 按右鍵邊	5日、「「「「「「」」。	攵・			
5.3 於 Enabled 按右鍵選	「「」」				
5.3 於 Enabled 按右鍵邊 底數為十六進位之數值:	皆 実 修 は の で 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	외, 數值設定為	ы <mark>1</mark> · 按確定	0	
5.3 於 Enabled 按右鍵邊 底數為十六進位之數值	皆 握 修 は の で の が の が の が の や の や の や の や の や の や の や	외· 數值設定為	å <mark>1</mark> ⋅按確定	٥	
5.3 於 Enabled 按右鍵邊 底數為十六進位之數值	皆 握 修 は の が の で が の が の で 、 の 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	⊈ 數值設定為 	₿ <mark>1</mark> ·按確定	٥	
5.3 於 Enabled 按右鍵邊 底數為十六進位之數值 ¹¹ DWORD (32-位元) 值 ¹¹ 值名稱(N):	選擇修改 資料・	외· 數值設定為 ──×	ы́┨·按確定	۰	
5.3 於 Enabled 按右鍵邊 底數為十六進位之數值 ¹¹¹ DWORD (32-位元) 值 ¹¹² de X編(N): nabled	援援(修改) 资料, 资料,	외・ 數值設定為 ──×	ы┨·按確定	°	

1.6 設定完成後,請重新啟動主機,使設定生效。

● 十六進位(H)
 ○ 十進位(D)

確定

取消

2 · Apache

2.1 開啟 Apache 設定檔

Apache SSL 協定設定值儲存於 Apache 設定檔內

(依 Apache 版本不同可能存放於 httpd.conf、httpd-ssl.conf 或 ssl.conf)



2.2 搜尋 SSLProtocol 參數

尋找		×
尋找目標(N): SSLProte	col	技下一個任
□ 大小寫視為相異(C)	搜尋方向 〇 向上① ④ 向下①	取消

2.3 修改 SSLProtocol 參數內容

設定 SSL 協定。可以用『+、-』分別表示『允許、拒絕』某些特定的協定。

SSLProtocol -all +TLSv1.2 (即代表允許 TLS 1.2, 並拒絕其他較過時的協定)

SSLProtocol -all +TLSv1.2

備註:如需同時允許多個協定,請在最後面加上協定名稱(每個協定要用空格間隔) SSLProtocol -all +TLSv1 +TLSv1.1 +TLSv1.2

```
(代表同時允許 TLS 1.0、TLS 1.1、TLS 1.2 傳輸協定)
```

2.4 設定完成後請儲存檔案,並重新啟動 Apache 服務,使設定生效。

3 · Tomcat

3.1 開啟 Tomcat 設定檔

Tomcat SSL 協定設定值儲存於 Tomcat 設定檔內 (預設路徑為\$TOMCAT HOME \conf 目錄下的 server.xml 檔案)

3.2 開啟 Tomcat 設定檔 server.xml, 並搜尋「sslProtocol」字串, 可找到其中跟 SSL 相

```
關的設定值
```

server.xml - 記事本	X
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)	
Define a SSL HTTP/1.1 Connector on port 8443<br This connector uses the JSSE configuration, when using APR, the connector should be using the OpenSSL style configuration described in the APR documentation>	-
<connector <br="" port="443" protocol="HTTP/1.1" sslenabled="true">maxThreads="150" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="c:\mykeystore.jks" keyAlias="keyname" keystorePass="xxx" /></connector>	•

3.3 如為 Tomcat 5 或 Tomcat 6 (6.0.38 前版本)

請新增「sslProtocols」設定, sslProtocols="TLSv1.2"



備註:如需同時允許多個協定,請在最後面加上協定名稱(每個協定要用,間隔)

sslProtocols="TLSv1,TLSv1.1,TLSv1.2"

(代表同時允許 TLS 1.0、TLS 1.1、TLS 1.2 傳輸協定)

請新增「sslEnabledProtocols」設定, sslEnabledProtocols="TLSv1.2"



備註:如需同時允許多個協定,請在最後面加上協定名稱(每個協定要用,間隔)

sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

(代表同時允許 TLS 1.0、TLS 1.1、TLS 1.2 傳輸協定)

3.5 設定完成後請儲存檔案,並重新啟動 Tomcat 服務,使設定生效。