KG Inicis

보안취약 프로토콜
서비스 전환 가이드

Ver. 1.0

1. 보안취약 프로토콜 서비스 전환 안내

SSL 프로토콜에 대한 보안취약점(POODLE, Padding Oracle on Downgraded Legacy Encryption)이 발견됨에 따라 당사 전자결제서비스의 보안 강화 및 정보보호를 위하여 보안 프로토콜 개선이 진행되고 있습니다.

▣ 작업 배경

- 구)보안 프로토콜의 대표적인 보안취약점 (일명 POODLE, Padding Oracle on Downgraded Legacy Encryption) 및 TLS 1.0의 암호화 알고리즘 취약점으로 인해 중간자 공격(MITM)을 통해 주요 고객정보유출 문제점 지속 (2014년 부터~)
- KG이니시스는 다중 암호화를 통해 보안성을 유지하여 (TLS1.0, 1.1)을 부분 허용하고 있으나, 향후 신뢰성 있는 서비스를 위하여, TLS 1.2 프로토콜 전용 서비스로 완전 전환을 추진 중

▣ 지원종료 일정

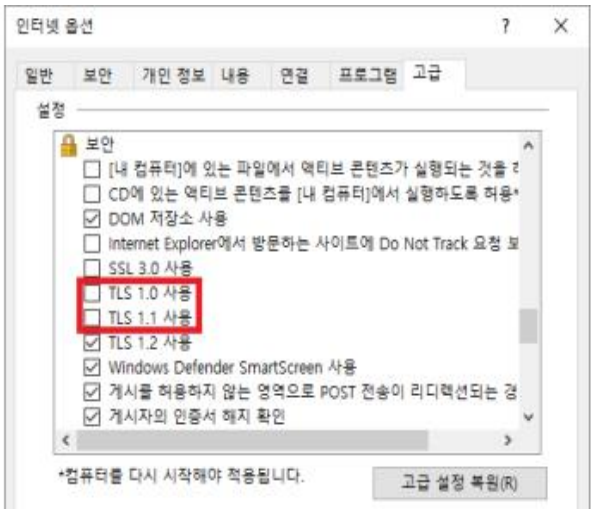
- 각 브라우져 벤더의 서비스 종료 일정에 따라, TLS1.0, TLS1.1 프로토콜이 차단될 예정
- 세부 일정은 브라우저 사 사정에 따라 변동될 수 있음

브라우저	TLS 종료 일정
Chrome	2020년 1월
IE, Edge	2020년 상반기
Safari	2020년 3월
Firefox	2020년 3월

2. 서비스 종료 영향

▣ 영향도

- 사용자(고객) : IE10 이하 버전을 통하여 결제 시도 시 오류 발생
  ※ 인터넷옵션 → 고급 → TLS1.2를 제외한 모든 프로토콜 사용해제



• KG이니시스 가맹점 : TLS 1.2 이상을 지원하지 않는 서버, 라이브러리 업그레이드 필요
※ 브라우저, 운영체제, 라이브러리, WEB/WAS 지원환경 확인요망

▶ 브라우저별 SSL프로토콜 지원여부

종류		Internet Explorer							Chrome				FireFox	
버전		4~5	6	7	8	9	10	11	~21	~29	~39	40~	27~	34~
SSL 프로토콜	SSL 2.0	O	O	X	X	X	X	X	X	X	X	X	X	X
	SSL 3.0	O	O	O	O	O	O	O	O	O	O	X	O	X
	TLS 1.0	X	X	O	O	O	O	O	O	O	O	O	O	O
	TLS 1.1	X	X	X	O	O	O	O	X	O	O	O	O	O
	TLS 1.2	X	X	X	O	O	O	O	X	X	O	O	O	O

참고 : https://en.wikipedia.org/wiki/Transport_Layer_Security

▶ 운영체제(OS)별 SSL프로토콜 지원여부

종류		Windows XP Server 2003	Windows Vista Server 2008	Windows 7 Server 2008 R2	Windows 8 Server 2012	Windows 8.1 Server 2012 R2	Windows 10 Server 2016
SSL 프로토콜	SSL 2.0	O	O	O	O	O	O
	SSL 3.0	O	O	O	O	O	O
	TLS 1.0	O	O	O	O	O	O
	TLS 1.1	X	X	O	O	O	O
	TLS 1.2	X	X	O	O	O	O

종류		Android			iOS			OS X		
버전		~4.0	4.1~ Jelly Been	5.1~ Lollipop	1~4	5~	9~	~10.8	10.9~	10.11~
SSL 프로토콜	SSL 2.0	X	X	X	X	X	X	X	X	X
	SSL 3.0	O	O	X	O	O	X	O	O	X
	TLS 1.0	O	O	O	O	O	O	O	O	O
	TLS 1.1	X	O	O	X	O	O	X	O	O
	TLS 1.2	X	O	O	X	O	O	X	O	O

▶ 라이브러리 SSL프로토콜 지원여부

종류		Open SSL		JAVA			Mozilla NSS		
버전		0.9.8~	1.0.1~	JDK 6	JDK 6_111	JDK 7	3.13	3.14	3.15
SSL 프로토콜	SSL 2.0	X	X	X	X	X			
	SSL 3.0	O	O	O	O	O			
	TLS 1.0	O	O	O	O	O	O	O	O
	TLS 1.1	X	O	X	O	O	X	O	O
	TLS 1.2	X	O	X	X	O	X	X	O

참고 : https://blogs.oracle.com/java-platform-group/entry/diagnosing_tls_ssl_and_https

▶ 서버 SSL프로토콜 지원여부

종류		Apache		Tomcat	IBK Server		Microsoft IIS	NginX
버전		~ 2.2.22	2.2.23 ~	-	~ GSKit 7	GSKit 8 ~	-	-
SSL 프로토콜	SSL 2.0	O	O	JAVA 버전에 따름	O	O	Windows Server 버전에 따름	OpenSSL 버전에 따름
	SSL 3.0	O	O		O	O		
	TLS 1.0	O	O		O	O		
	TLS 1.1	X	O		X	O		
	TLS 1.2	X	O		X	O		

종류		Oracle Weblogic			Oracle HTTP Server		WebToB	
버전		JSSE 사용	~ 11	~ 12	~ 11.1.1.8	11.1.1.9 ~	~ 4.1.5.2	4.1.5.3 ~
SSL 프로토콜	SSL 2.0	JAVA 버전에 따름	X	X	X	X	O	O
	SSL 3.0		O	O	O	O	O	O
	TLS 1.0		O	O	O	O	O	O
	TLS 1.1		X	O	X	O	X	O
	TLS 1.2		X	O	X	O	X	O

참고 :
http://www.ibm.com/support/knowledgecenter/SS7K4U_8.0.0/com.ibm.websphere.ihs.doc/info/ihs/ihs/cihs_newfunction.html

참고 : https://technet.tmaxsoft.com/upload/download/online/webtob/pver-20150203-000001/release-note/ver_4_1_5_3.html

▣ 적용 대상 서비스

• 당사에서 제공하는 결제서비스 모듈에는 아래와 같이 TLS1.2가 이미 적용된 상태입니다.

서비스 모듈	서비스도메인	프로토콜	지원여부
PC 웹 표준	https://stdpay.inicis.com https://fcstdpay.inicis.com https://ksstdpay.inicis.com	TLS 1.2	O
모바일	https://mobile.inicis.com https://fcmobile.inicis.com https://ksmobile.inicis.com	TLS 1.2	O
INILITE	https://inilite.inicis.com	TLS 1.2	O
INIAPI	https://iniapi.inicis.com	TLS 1.2	O
플러그인	https://plugin.inicis.com	TLS 1.2	O

※ TX 모듈 (INIpay50, 41, 45)의 경우 socket 을 통한 TCP IP 통신하는 모듈이므로, 프로토콜의 영향을 받지 않음

3. 기술 지원 문의

문의처 : **02-3430-5960** (ts@inicis.com)

-끝-