KG Inicis

보안취약 프로토콜
서비스 전환 가이드

Ver. 1.1

개 정 이 력

버전	작성일	변경내용[1]	작성자	승인자
1.0	2019-11-19	최초 작성	기술지원	
1.1	2020-05-11	Plug-in (activeX) TLS1.2 지원 중지 추가	기술지원	

[1] 변경 내용: 변경이 발생되는 위치와 변경 내용을 자세히 기록(변경 페이지 및 변경 내용을 기술한다.)

목 차

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

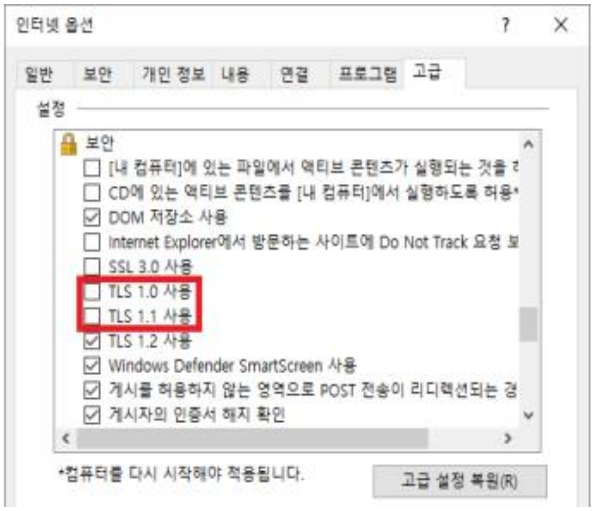
- 각 브라우져 벤더의 서비스 종료 일정에 따라, TLS1.0, TLS1.1 프로토콜이 차단될 예정
- 세부 일정은 브라우저 사 사정에 따라 변동될 수 있음

브라우저	TLS 종료일정
Chrome	Chrome83 출시 이후 차단 (5 월 예정)
IE, Edge	9 월
Safari	상반기
Firefox	상반기

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~ Loilpop	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.
(단, 플러그인/Plug-in 모듈은 2020년06월30일 지원 종료)

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
INI-API	https://iniapi.inicis.com	TLS 1.2	O
플러그인 사용 결제 창 모듈	https://plugin.inicis.com *결제 창 호출 시 위 도메인 사용 activeX모듈	TLS 1.2	X

※ TX 모듈 (INIpay50, 41, 45)의 경우 socket 을 통한 TCP IP 통신하는 모듈이므로, 프로토콜의 영향을 받지 않음 *** 참고 : TX 모듈중 결제창을 띄우지 않는 모듈에 한함**

※ 가맹점 서버에 TLS1.2 프로토콜 적용 후, 테스트 결제를 진행하여 정상적용 여부 확인 필요

- 계속 -

▣ Pulg-IN 서비스 지원중지

Plug-In 서비스는 2020년 6월 30일을 기점으로 서비스 지원을 종료할 예정이오니 웹표준 결제창으로 전환하여 주시기 바랍니다.

- **(정부권고)** 과학기술정보통신부 국정과제 33-2('20년까지 민간 500대 웹사이트의 액티브X 제거)
- **(고객감소)** Pulg-IN 서비스는 설치문제, 오류증가, TLS1.2미지원으로 보안성 감소 등 다양한 문제점으로 웹사이트의 경쟁력 저하

웹 표준 결제창 전환시에는 다음과 같은 장점이 있습니다.

- **(고객확대)** IE뿐만 아니라 크롬등 모든 브라우저를 지원하기 때문에 사용자 결제 건수가 증가합니다.
- **(편의성 향상)**설치없이 바로 결제가 가능해짐에 따라 결제시간 단축 등 고객만족도가 향상됩니다.
-

1. 다양한 간편결제 지원
   - **삼성페이, 페이코, 카카오페이, Lpay, SSGpay 등 지원**
2. 웹 접근성(장애인 차별 금지법) 지원
   - **국가 권고 사항인 장애인 차별 금지법 웹표준 지원**
3. 다국어 지원
   - **증가하는 해외 거래를 위한 한국어 / 영어 / 중국어 지원**
4. 기존 결제창(ActiveX기반 플러그인) 대비 높은 결제 성공율
   - **기존 결제창 : 인증대비 승인 약 (80%), 현재 웹표준 결제창 (95%)**

▣ 플러그인(activeX) 사용 결제 창 모듈의 대체 모듈 안내

서비스 종료 모듈	서비스 종료 도메인	대체모듈
INILite INIpay4x INIpay50	https://plugin.inicis.com *결제 창 호출시 위 도메인 사용시	**웹표준 통합 결제 창 사용** https://manual.inicis.com/stdpay/
INIpay41(빌링인증)	https://plugin.inicis.com *빌링 인증 창 호출시 위 도메인 사용시	**웹표준 빌링 인증 창 사용 (빌링키 발급 부분)** https://manual.inicis.com/stdpay/
에스크로구매결정	https://plugin.inicis.com *구매 결정 창 호출시 위 도메인 사용시	**웹표준 모듈 내 구매결정 사용 (에스크로 구매 확인 부분)** https://manual.inicis.com/stdpay/

3. 기술 지원 문의

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

-끝-