U+ Biz
New Biz. Practice Creator

LG U+

보안 취약 프로토콜 단계별 개선 안내

목 차

2017. 3

LG U+ 전자결제

보안 취약 프로토콜 단계별 개선 안내

❑ 배경

■ http (HyperText Transfer Protocol)
- 인터넷 웹서버와 사용자의 브라우저/서버의 통신을 위한 규약

■ https (HyperText Transfer Protocol over Secure Soket Layer)
- http + 전송되는 내용을 암호화 하여 전송하며 보안상 http보다 안전 (결제 연동규격서에 HPPS로 연동 명시)

[HTTPS 프로토콜]

■ SSL(Secure Socket Layer)
- 배경 : 1993년 웹서버와 브라우저간의 안전한 통신을 위해 Netscape社에 의해 개발됨
- 특징 : 세션계층에서 적용되며, 응용계층의 FTP, Telnet, Http등의 프로토콜의 안전성 보장
- 지원프로토콜 : HTTP(HTTPS:443), TELNET(TELNETS:992), POP3(POP3S:995), FTP, NNTP, etc.
- 주요기능 : 서버 인증, 클라이언트 인증, 기밀성 보장
- 버전 history : SSL2.0 → SSL3.0

■ TLS(Transport Layer Security)
- 배경 : SSL3.0이 표준화된 이후 IETF는 1996년 6월부터 TLS프로토콜에 대한 표준화(SSL v3.1)
- 특징 : SSL3.0을 기반으로 한 업그레이드 프로토콜
- 버전 : TLS1.0 → TLS1.1 → TLS1.2

보안 취약 프로토콜 단계별 개선 안내

❑ 이슈

✓ SSL2.0 / SSL3.0 보안취약 – POODLE 공격

암호화 프로토콜인 SSL3.0 은 일명 푸들(POODLE, Padding Oracle on Downgraded Legacy Encryption)이라는 취약점이 확인되었습니다.

'푸들(Poodle)'이라는 이 취약점은 18년 된 SSL3.0(Secure Socket Layer)에서 발견된 새로운 보안 취약점으로 데이터 보안을 위해 전송 하는 데이터의 암호화 기술이 취약점에 의하여 암호화 가 풀려 해커에게 노출된다는 취약점입니다.

✓ **보안 취약 암호화 프로토콜 차단**

KISA 지침에 따라 오래된 암호화 프로토콜인 SSL2.0 / SSL3.0 차단하고 TLS 프로토콜만 허용

HTTPS 를 무조건 사용해야 하며 HTTPS에서도 SSL2.0 / SSL3.0 차단 및 **TLS 1.0 / 1.1 / 1.2 만 허용** (*허용기준 참조)

LG U+는 **'16년 SHA2 인증서 업데이트를 진행한 바, SSL3.0까지 차단하더라도 기존 고객사 단말/서버에 큰 영향 없음**

현재	변경	
암호화 프로토콜	암호화 프로토콜	비고
SSL 2.0	-	차단
SSL 3.0	-	차단
TLS 1.0	TLS 1.0	허용
TLS 1.1	TLS 1.1	허용
TLS 1.2	TLS 1.2	허용

보안 취약 프로토콜 단계별 개선 안내

❑ 영향

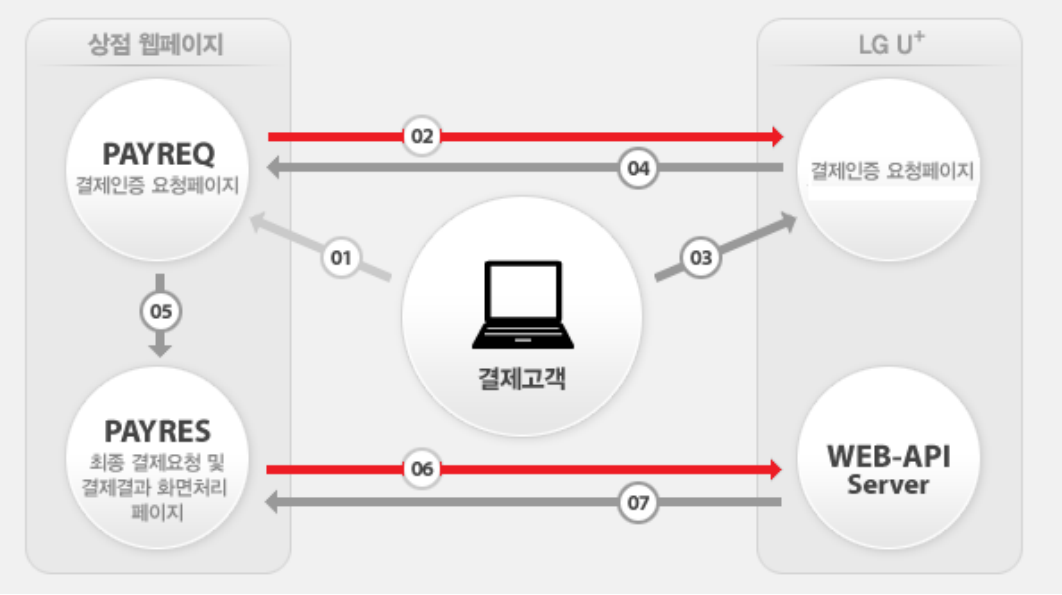
■ 결제고객

구 IE 브라우저 버전의 경우 결제창이 호출되지 않음 **(결제창 호출불가)**

TLS1.0이상을 지원하는 IE브라우저라고 하더라도 브라우저 default 설정이 아니므로
고객이 직접 브라우저의 설정을 변경해야 결제창이 호출됨 (IE버전에 따라 동작 상이)

■ 고객사

고객사의 결제 서버가 TLS를 지원하지 않는 서버인 경우 통신 불가 : 고객사에서 서버 업그레이드 필요
(결제 승인시 고객사 서버 => 유플러스 서버간 통신 불가)
→ LG U+는 **'16년 SHA2 인증서 업데이트를 진행한 바, SSL3.0까지 차단하더라도 기존 고객사 단말/서버에 큰 영향 없음**



[결제/승인 프로세스]

※ https 통신은 아래 두 단계에서 진행됨.
(왼쪽 붉은 화살표)

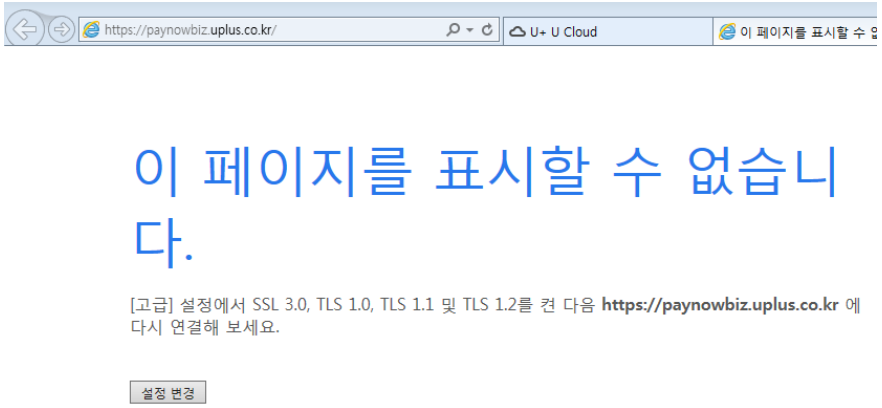
② 결제창 호출 단계
⑥ 결제 요청 단계(고객사 서버 -> LG U+ 서버)

보안 취약 프로토콜 단계별 개선 안내

❑ 오류 및 조치

[오류]
구 브라우저 또는 신 브라우저라도 TLS가 허용되어 있지 않으면 오류가 발생합니다.
* 구 브라우저와 최신 브라우저의 차이는
최신 브라우저의 경우(IE 8이상) TLS가 기본적으로 사용으로 체크되어 있기 때문에 오류가 발생할 여지가 작으나,
구 브라우저는 SSL2.0 / SSL3.0만 사용으로 체크되어 있고, TLS1.0부터 1.2는 사용으로 설정 되어 있지 않은 경우가 있어
구 브라우저를 사용하는 고객이 결제창이 뜨지 않고 하단의 오류메시지만("이 페이지를 표시할 수 없습니다.") 표기됨

단, 신 브라우저라고 하더라도
사용자가 강제로 브라우저의 옵션을 조정하였거나 기타 프로그램들에 의하여 인터넷설정이 TLS가 미사용으로 변경되었다면
결제창이 뜨지 않고 "이 페이지를 표시할 수 없습니다." 라는 화면이 표기됨



[오듀메시지 화면]

종류	버전	SSL Protocol				
		SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Internet Explorer	4, 5	지원	지원	미지원	미지원	미지원
	6	지원	지원	미지원	미지원	미지원
	7	미지원	지원	지원	미지원	미지원
	8	미지원	지원	지원	지원	지원
	9	미지원	지원	지원	지원	지원
	10	미지원	지원	지원	지원	지원
	11	미지원	지원	지원	지원	지원
Chrome	~ 21	미지원	지원	지원	미지원	미지원
	~ 29	미지원	지원	지원	지원	미지원
	~ 39	미지원	지원	지원	지원	지원
	40 ~	미지원	미지원	지원	지원	지원
FireFox	27 ~	미지원	지원	지원	지원	지원
	34 ~	미지원	미지원	지원	지원	지원
Safari	-	iOS, OS X 버전에 따름				

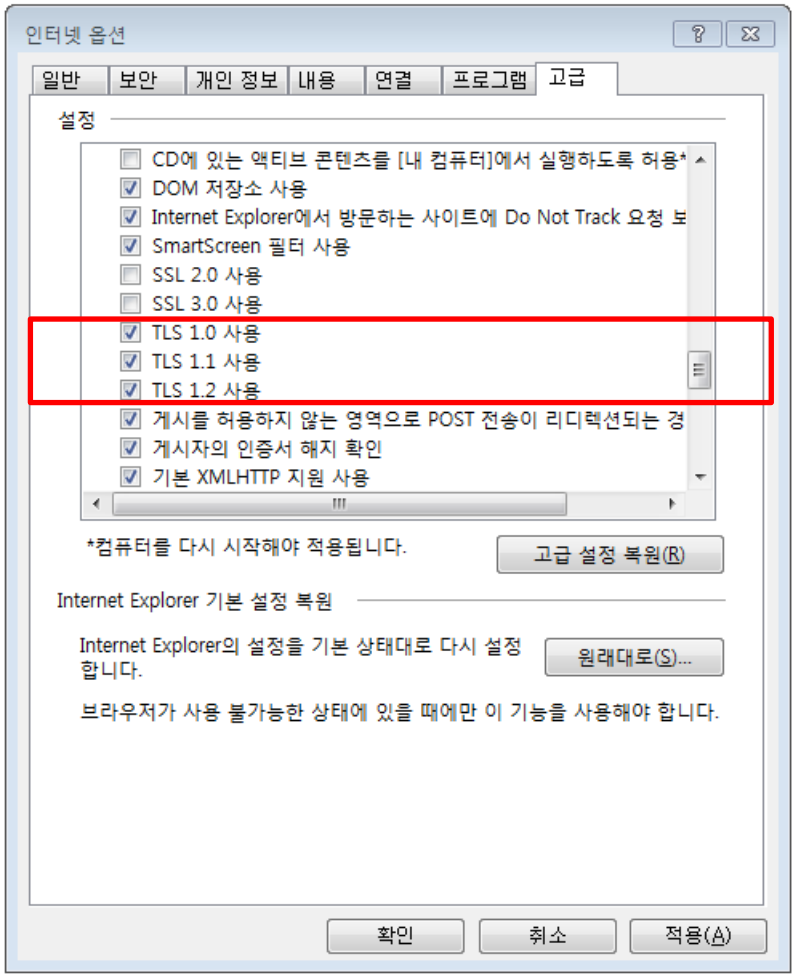
[SSL 프도도콛 지원환경]

보안 취약 프로토콜 단계별 개선 안내

❑ 오류 및 조치

[결제고객 조치]
결제창이 뜨지 않고 **"이 페이지를 표시할 수 없습니다."**라는 화면이 표기됨

인터넷옵션 → 고급 → TLS1.0 / TLS1.1 / TLS1.2 사용 설정



보안 취약 프로토콜 단계별 개선 안내

❑ 당사 보안 취약 프로토콜 업데이트 일정

- 보안 취약 프로토콜 SSL2.0 / 3.0 차단 관련하여 당사 각 WEB서버 설정 변경 작업을 **2017년 3월 23일부터 순차적으로 적용**할 예정임.

- **주요 Domain 안내**

도메인	구분	적용계획	비고
xpay.lgdacom.net:7443 xpayclient.lgdacom.net:7443	전자결제 테스트	03월 23일	전자결제 연동 고객사 테스트 용도
pg.dacom.net	1.0 (MServer 포함)	3월 30일 ~ 4월 27일	순차 적용 예정
xpay.lgdacom.net xpayclient.lgdacom.net	2.0 일반	3월 30일 ~ 5월 11일	순차 적용 예정
pgdownload.uplus.co.kr	다운로드 웹 서버	3월 30일 ~ 4월 27일	순차 적용 예정

- **전자결제 기술지원 문의** : 1644-3217, paytech@lguplus.co.kr

- **전자결제 고객센터 : 1544-7772**

별첨. SSL Protocol 지원 환경 정보 안내

한국정보인증을 비롯한 각 기관에서 권장하는 SSL Protocol 은 **TLS1.0 / TLS1.1 / TLS1.2 이며**
SSL 2.0 / SSL3.0 은 POODLE 취약점 등의 이유로 사용이 권장되지 않습니다.
따라서 아래의 정보를 참고하시어 각 운영 환경에 맞는 SSL Protocol 설정을 하시기 바랍니다.

❑ 브라우저

종류	버전	SSL Protocol				
		SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Internet Explorer	4, 5	지원	지원	미지원	미지원	미지원
	6	지원	지원	미지원	미지원	미지원
	7	미지원	지원	지원	미지원	미지원
	8	미지원	지원	지원	지원	지원
	9	미지원	지원	지원	지원	지원
	10	미지원	지원	지원	지원	지원
	11	미지원	지원	지원	지원	지원
Chrome	~ 21	미지원	지원	지원	미지원	미지원
	~ 29	미지원	지원	지원	지원	미지원
	~ 39	미지원	지원	지원	지원	지원
	40 ~	미지원	미지원	지원	지원	지원
FireFox	27 ~	미지원	지원	지원	지원	지원
	34 ~	미지원	미지원	지원	지원	지원
Safari	-	iOS, OS X 버전에 따름				

[참고]

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

❑ 운영체제

OS	SSL Protocol				
	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Windows XP / Server 2003	지원	지원	지원	미지원	미지원
Windows Vista / Server 2008	지원	지원	지원	미지원	미지원
Windows 7 / Server 2008 R2	지원	지원	지원	지원	지원
Windows 8 / Server 2012	지원	지원	지원	지원	지원
Windows 8.1 / Server 2012 R2	지원	지원	지원	지원	지원
Windows 10 / Server 2016	지원	지원	지원	지원	지원

종류	버전	버전명	SSL Protocol				
			SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Android	~ 4.0		미지원	지원	지원	미지원	미지원
	4.1 ~	Jelly Bean	미지원	지원	지원	지원	지원
	5.1 ~	Lolipop	미지원	미지원	지원	지원	지원

종류	버전	SSL Protocol				
		SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
iOS	1 ~ 4	미지원	지원	지원	미지원	미지원
	5 ~	미지원	지원	지원	지원	지원
	9 ~	미지원	미지원	지원	지원	지원
OS X	~ 10.8	미지원	지원	지원	미지원	미지원
	10.9 ~	미지원	지원	지원	지원	지원
	10.11 ~	미지원	미지원	지원	지원	지원

별첨. SSL Protocol 지원 환경 정보 안내

한국정보인증을 비롯한 각 기관에서 권장하는 SSL Protocol 은 **TLS1.0 / TLS1.1 / TLS1.2 이며**
SSL 2.0 / SSL3.0 은 POODLE 취약점 등의 이유로 사용이 권장되지 않습니다.
따라서 아래의 정보를 참고하시어 각 운영 환경에 맞는 SSL Protocol 설정을 하시기 바랍니다.

❑ 라이브러리

종류	버전	SSL Protocol				
		SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
OpenSSL	0.9.8 ~	미지원	지원	지원	미지원	미지원
	1.0.1 ~	미지원	지원	지원	지원	지원
JAVA	JDK 6	미지원	지원	지원	미지원	미지원
	JDK 6_111	미지원	지원	지원	지원	미지원
	JDK 7 ~	미지원	지원	지원	지원	지원
Mozilla NSS	3.13	정보없음	정보없음	지원	미지원	미지원
	3.14	정보없음	정보없음	지원	지원	미지원
	3.15	정보없음	정보없음	지원	지원	지원

[참고]

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

https://www.openssl.org/news/openssl-1.0.1-notes.html

❑ 서버

종류	버전	SSL Protocol				
		SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Apache	~ 2.2.22	지원	지원	지원	미지원	미지원
	2.2.23 ~	지원	지원	지원	지원	지원
Tomcat	-	JAVA 버전에 따름				
IBM Server	~ GSKit 7	지원	지원	지원	미지원	미지원
	GSKit 8 ~	지원	지원	지원	지원	지원
Microsoft IIS	-	Windows Server 버전에 따름				
NginX	-	OpenSSL 버전에 따름				
Oracle Weblogic	JSSE 사용	JAVA 버전에 따름				
	~ 11	미지원	지원	지원	미지원	미지원
	12 ~	미지원	지원	지원	지원	지원
Oracle HTTP Server	~ 11.1.1.8	미지원	지원	지원	미지원	미지원
	11.1.1.9 ~	미지원	지원	지원	지원	지원
WebToB	~ 4.1.5.2	지원	지원	지원	미지원	미지원
	4.1.5.3 ~	지원	지원	지원	지원	지원

[참고]

http://www.apache.org/dist/httpd/CHANGES_2.2

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

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

FAQ.

Q. 구 IE 브라우저 버전의 경우 결제창이 호출되지 않는다고 하는데, 구 IE 브라우저 버전은 어떻게 되나요?
A. IE 8미만, 즉 TLS가 지원하지 않는 브라우저의 경우에 해당됩니다. (*SSL 프로토콜 지원환경 참조)

Q. 신 브라우저의 경우(IE 8이상)에도 결제창 호출이 되지 않는 경우가 있나요?
A. 사용자가 강제로 브라우저의 옵션을 조정하였거나 기타 프로그램들에 의하여 인터넷설정이 TLS가 미사용으로 변경되었다면 결제창이 뜨지 않고 "이 페이지를 표시할 수 없습니다."라는 화면이 표기됨
그럴 경우 사용자의 브라우저에서 인터넷옵션 → 고급 → TLS1.0 / TLS1.1 / TLS1.2 사용 설정 하시기 바랍니다.

Q. 정확히 언제부터 적용되나요?
A. 보안 취약 프로토콜 SSL2.0 / 3.0 차단 관련하여 당사 각 WEB서버 설정 변경 작업을 2017년 3월 23일 부터 순차적으로 적용할 예정이며 2017년 7월 부터는 TLS 설정된 브라우저에서만 결제가 가능합니다.

Q. 쇼핑몰(고객사)에서 조치해야 될 사항이 있나요?
A. 고객사의 결제 서버가 TLS를 지원하지 않는 서버인 경우 통신이 불가하며 고객사에서 서버 업그레이드가 필요합니다.
(결제 승인시 고객사 서버 => 유플러스 서버간 통신 불가)
하지만, 당사는 SSL2.0 / SSL3.0 차단 진행하더라도 '16년 적용한 SHA2 인증서의 지원 단말/서버에 모두 허용되어 고객사에는 큰 이슈 없습니다.

Q. 기술 관련 사항으로 문의할 점이 있습니다. 어디에 연락하면 되나요?
A 전자결제 기술지원(paytech@lguplus.co.kr, 1644-3217)로 문의하시면 됩니다.