

# 보안 취약 프로토콜/알고리즘 차단 안내

## 목 차

1. 개요
  2. 차단 영향
  3. 오류 및 조치사항
  4. 테스트 환경 제공 안내
  5. FAQ
- 별첨. 닷넷(.NET) Framework Client 지원 환경 정보 안내  
별첨. SSL Protocol 지원 환경 안내

2018. 1  
LG U+ 전자결제

## □ 개요

### ■ 보안 취약점 발견(POODLE, DROWN 등)

- POODLE (Padding Oracle on Downgraded Legacy Encryption)  
데이터 보안을 위해 전송 데이터를 암호화하는 기술이 암호화가 풀려 해커에게 노출되는 취약점
- DROWN (Decrypting RSA with Obsolete and Weakened eNcryption)  
같은 키를 사용하는 SSL 서버의 연결을 악용, TLS연결을 가로채는 취약점

### ■ 보안 취약 프로토콜/알고리즘 차단 진행

- POODLE, DROWN 등의 취약점은 서버가 오래된 프로토콜/알고리즘을 지원하는 점을 악용함
- 이에 대응하기 위하여 LG U+ 전자결제에서는 취약한 프로토콜 및 알고리즘에 대하여 차단 진행
- 고객/고객사의 충분한 준비 시간 확보를 위하여 3차례에 걸쳐 차단 진행 예정

### ■ 1차 차단 : 작업 연기 (추후 일정 재공지 예정)

- 차단 프로토콜 : SSL 3.0 (TLS 1.0 이상 사용 가능)
- 차단 알고리즘 : RC2, RC5, RC6, DES, 2DES, 3DES

### ■ 2차 차단 : 작업 연기 (추후 일정 재공지 예정)

- 차단 프로토콜 : SSL 3.0 및 TLS 1.0 (TLS 1.1 이상 사용 가능)
- 차단 알고리즘 : RC2, RC5, RC6, DES, 2DES, 3DES 및 RC4, MD4, MD5

### ■ 3차 차단 : 작업 연기 (추후 일정 재공지 예정)

- 차단 프로토콜 : SSL 3.0, TLS1.0 및 TLS 1.1 (최종 TLS 1.2 이상 사용 가능)
- 차단 알고리즘 : RC2, RC5, RC6, DES, 2DES, 3DES, RC4, MD4, MD5 및 SHA1

### ■ 전자결제 기술지원 (1644-3217, [paytech@lguplus.co.kr](mailto:paytech@lguplus.co.kr)), 전자결제 고객센터 (1544-7772)

## □ 차단 영향

현재	변경		
암호화 프로토콜	암호화 프로토콜	허용여부	차단 일정
SSL 2.0	-	차단	18/02/27 (화)
SSL 3.0	-	차단	
TLS 1.0	-	차단	18/04/26 (목)
TLS 1.1	-	차단	18/06/26 (화)
TLS 1.2	TLS 1.2	허용	

### ■ 결제고객

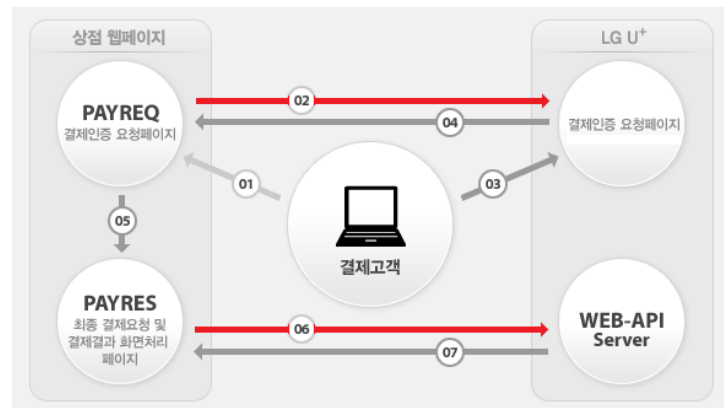
- 구 IE 브라우저 버전의 경우 결제창이 호출되지 않음 (결제 오류 발생)  
 ※ 브라우저 default 설정에 따라 고객이 직접 브라우저의 설정을 변경해야 결제창이 호출됨 (IE10이하 버전)

### ■ 고객사

- 고객사의 결제 서버가 상위 알고리즘을 지원하지 않는 서버인 경우 고객사<-> 유플러스 서버 간 통신 불가(결제 오류 발생)  
 ※ 고객사 서버 업그레이드 필요

### ■ 결제/승인 프로세스

- 서버 간 https 통신은 아래 두 단계를 통해 진행됨(② 결제창 호출 단계, ⑥ 결제 요청 단계(고객사 서버 -> LG U+ 서버))



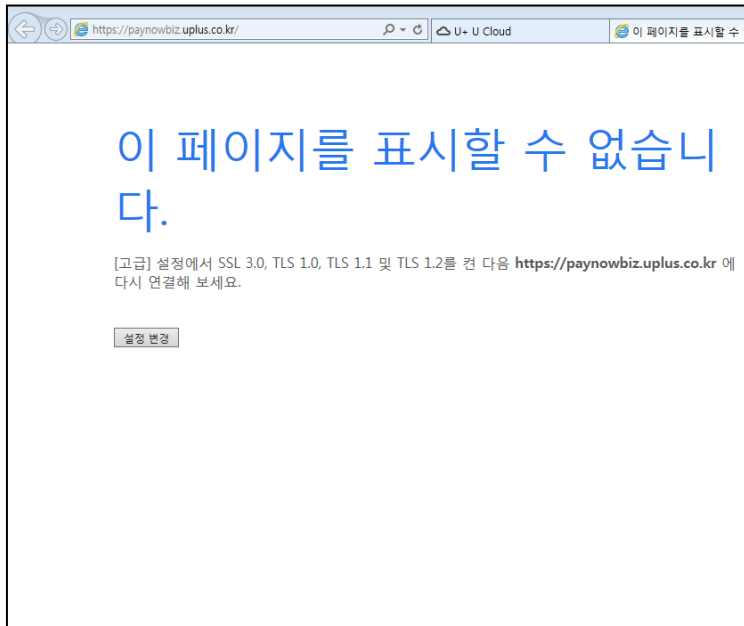
## □ 오류 및 조치사항

### ■ 결제고객 브라우저 오류

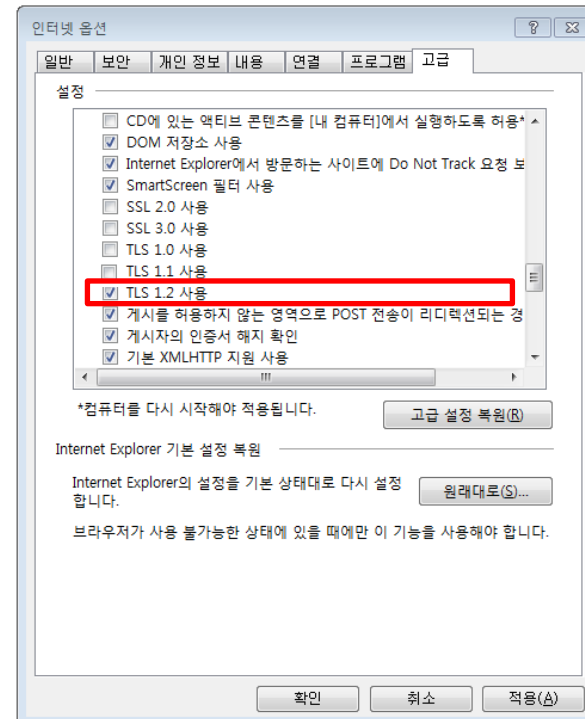
- 내용: IE10 이하 버전을 통하여 결제 시도 시 오류 발생 가능 (아래 화면 참조 요망)
- 사유: IE10 이하 버전에서는 보안 프로토콜 기본 설정 상태가 TLS1.1, TLS1.2 미사용 상태
- 조치사항: 인터넷옵션 → 고급 → TLS1.2 사용 설정

※ 최신 브라우저에서도 사용자가 강제로 옵션 조정하였거나, 기타 다른 프로그램에 의하여 설정이 변경되었다면 오류 발생 가능

### ■ 오류 예시 화면



### ■ 조치사항



## □ 테스트 환경 제공 안내

### ■ 테스트 URL 제공

- 보안 취약 프로토콜/알고리즘 차단 이전 고객사에서 사전 테스트를 진행하실 수 있도록 테스트 URL을 별도 제공함
- 고객사 담당자께서는 차단 적용 이전 반드시 테스트 URL을 이용하여 **사전 테스트 진행 요청**

※ TLS 1.2 (TLS 1.1까지 차단)된 환경에 대해서 테스트 진행이 가능합니다.

### ■ 조치사항

- 조치 1 : payreq 샘플파일에서 xpay.js 또는 xpay\_crossplatform.js 의 도메인 정보 변경 (고객 브라우저 테스트)

기존: [https://xpay.uplus.co.kr/xpay/js/xpay\\_crossplatform.js](https://xpay.uplus.co.kr/xpay/js/xpay_crossplatform.js) (또는 xpay.js)  
변경 후: [https://xpay.uplus.co.kr:9443/xpay/js/xpay\\_crossplatform.js](https://xpay.uplus.co.kr:9443/xpay/js/xpay_crossplatform.js) (또는 xpay.js)

- 조치 2 : lgdacom.conf 파일에서 접속 도메인 정보를 변경 후 **해당 서버 재기동 수행 및 결제 테스트**

제공파일	제공파일설명
lgdacom/conf/lgdacom.conf	LG유플러스 환경파일

test\_url = <https://xpayclient.lgdacom.net:9443/xpay/Gateway.do>

- 전자결제 기술지원 문의: 1644-3217, paytech@lguplus.co.kr
- 전자결제 고객센터: 1544-7772

Q. 구 IE 브라우저 버전의 경우 결제창이 호출되지 않는다고 하는데, 구 IE 브라우저 버전은 어떻게 되나요?

A. IE 10 이하 브라우저의 경우 해당됩니다. ('오류 및 조치사항' 참조 요망)

Q. 신 브라우저의 경우에도 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 표기될 수 있습니다.

※ 사용자의 브라우저에서 인터넷옵션 → 고급 → TLS1.2 사용 설정 하시기 바랍니다.

Q. 정확히 언제부터 적용되나요?

A. 보안 취약 프로토콜/알고리즘 차단 작업을 2018년 2월, 4월, 6월 세 차례에 걸쳐 진행할 예정이었으나 **고객사의 충분한 준비 기간 확보를 위하여 2018년 4월 현재 연기된 상태입니다.** 추후 작업 재개될 예정이므로 반드시 사전에 대비하시기 바랍니다.

Q. 쇼핑몰(고객사)에서 조치해야 될 사항이 있나요?

A. 고객사의 결제 서버가 상위 프로토콜/알고리즘을 지원하지 않는 경우 통신이 불가하며 고객사에서 서버 업그레이드가 필요합니다.  
(결제 승인시 고객사 서버 => 유플러스 서버간 통신 불가)

Q. 기술 관련 사항으로 문의할 점이 있습니다. 어디에 연락하면 되나요?

A. 전자결제 기술지원([paytech@lguplus.co.kr](mailto:paytech@lguplus.co.kr), 1644-3217)로 문의하시면 됩니다.

## ■ 고객사 확인 및 변경사항

고객사와 유플러스간 통신을 위하여 설치하는 XpayClient.NET 버전을 사용하시는 고객사는 TLS1.2 통신을 위해서는 .NET Framework 4.5 이상 버전 사용이 필요합니다.

(고객사의 프로그램은 C#, ASP, NET 으로 구성되어 있으나 유플러스의 XPayClient COM 버전을 사용하는 경우는 제외)

- 고객사의 프로그램의 .NET Framework 빌드한 버전을 확인하여 TLS1.2를 지원하는 환경인지 확인
- 고객사 .NET Framework 버전에 따라 유플러스 XpayClient .NET 버전을 최신 버전으로 교체
- .NET Framework 상위버전으로 변경이 어려운 경우 유플러스 XpayClient를 Com 버전으로 교체

## ■ 고객사 확인 및 변경사항

.NET 프레임워크	지원프로토콜
.NET 4.6 이상	SSLv3 , TLS 1.0 , TLS 1.1 , TLS 1.2 (Default)
.NET 4.5	SSLv3 , TLS 1.0 , TLS 1.1 , TLS 1.2 (Not Default)
.NET 4.0	SSLv3 , TLS 1.0 , TLS 1.1
.NET 3.5 , 이하	SSLv3 , TLS1.0

- 전자결제 기술지원 문의 : 1644-3217, [paytech@lguplus.co.kr](mailto:paytech@lguplus.co.kr)
- 전자결제 고객센터 : 1544-7772

KISA, 한국정보인증을 비롯한 각 기관에서 권장하는 SSL Protocol 은 TLS1.2이며 TLS1.0/TLS1.1/SSL 2.0/SSL3.0 은 보안에 취약하여 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](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 ~	Lollipop	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



KISA, 한국정보인증을 비롯한 각 기관에서 권장하는 SSL Protocol은 TLS1.1 / TLS1.2이며 TLS1.0/SSL 2.0/SSL3.0 은 보안에 취약하여 사용이 권장되지 않습니다.

따라서 아래의 정보를 참고하시어 각 운영 환경에 맞는 SSL Protocol 설정을 하시기 바라며, 서버 별 상세 설정은 별첨된 한국정보인증의 서버별 Cipher Suite 설정 방법' 문서를 참고하시기 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://blogs.oracle.com/java-platform-group/entry/diagnosing_tls_ssl_and_https)

## □ 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]

[https://technet.tmaxsoft.com/upload/download/online/webtob/pver-20150203-000001/release-note/ver\\_4\\_1\\_5\\_3.html](https://technet.tmaxsoft.com/upload/download/online/webtob/pver-20150203-000001/release-note/ver_4_1_5_3.html)