

LG CNS

보안 취약 프로토콜 Upgrade 적용 가이드

Ver. 1.2

본 문서와 정보는 LG CNS 재산입니다. 또한, 모든 정보는 LG CNS 소유 정보이며, LG CNS의 사전 동의 없이 본 문서의 어떤 정보도 열람, 복사, 유용, 또는 타인과 공유되어서는 안됩니다.

본 문서의 정보는 변경될 수 있으며 변경 시, 본 문서는 수정될 것입니다. 본 문서의 내용에 관한 어떠한 의견이라도 귀하의 프로젝트 또는 사업 담당자에게 전달하여 주십시오.

개 정 이 력

[illegible]

목 차

1. 개요.....	4
1.1. 하위 버전의 보안 취약점 발견 (POODLE, DROWN 등)	4
1.2. 보안 취약 프로토콜/알고리즘 차단 진행	4
1.3. TLS 1.0 이하 버전 차단 적용 일정.....	4
1.4. 업그레이드 관련 기술 문의	4
2. 영향 범위 및 조치사항 - 결제 고객	4
2.1. 영향 범위.....	4
2.2. 조치사항	5
3. 영향 범위 및 조치사항 - 고객사(가맹점)	6
3.1. 영향 범위.....	6
3.2. 사용 언어 별 조치사항	6
3.2.1. JAVA(JSP).....	6
3.2.2. PHP.....	7
3.2.3. ASP	7
3.2.4. ASP.NET (C#).....	8
3.2.5. Python.....	9
3.3. 테스트 환경 제공 안내	9
4. FAQ.....	9

1. 개요

일반적으로 인터넷에서 정보를 암호화해서 송수신하기 위해 프로토콜, 알고리즘을 사용하고 있습니다. 해당 프로토콜, 알고리즘은 결함이나 취약성을 개선하기 위해 버전 업을 해왔으며, KISA, 한국정보인증, 각 서버/OS/브라우저 제조사에서도 하위 버전의 보안 취약 프로토콜, 알고리즘은 사용 중단 및 차단을 권고하고 있는 상황입니다.

따라서 LG CNS 에서도 2019년 7월 1일부터 TLS 1.1 버전 이상만을 허용하도록 조치 예정이며, 이 가이드를 참고하여 연동 해 주시기 바랍니다.

보안 취약 내용 및 차단 항목은 아래를 참고하시기 바랍니다.

1.1. 하위 버전의 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, TLS 연결을 가로채는 취약점

1.2. 보안 취약 프로토콜/알고리즘 차단 진행

- POODLE, DROWN 등의 취약점은 서버가 오래된 프로토콜을 지원하는 점을 악용함
- 이에 대응하기 위하여 LG CNS에서는 취약한 프로토콜에 대하여 차단 진행
- 차단 프로토콜 : SSL 3.0 이하, TLS 1.0 (TLS 1.1 이상 사용 가능)

1.3. TLS 1.0 이하 버전 차단 적용 일정

- 차단 프로토콜 : TLS 1.0 이하 버전 (TLS 1.1 이상 사용 가능)
- 고객사 업그레이드 완료 기한 : 2019년 6월 30일 일요일 까지
- TLS 1.0 이하 차단 적용 일시 : 2019년 7월 1일 월요일

1.4. 업그레이드 관련 기술 문의

- LG CNS 기술지원 담당
- tech.cns@lgcns.com / 02-2099-2385

2. 영향 범위 및 조치사항 - 결제 고객

2.1. 영향 범위

- IE10 이하 버전의 경우 Default 상태에서 결제창이 호출되지 않음 : 결제 오류 발생
- 고객이 직접 [2.2 조치사항] 내용과 같이 브라우저의 설정을 변경해야 결제창이 호출됨

- 오류 예시 화면 (고객 브라우저)

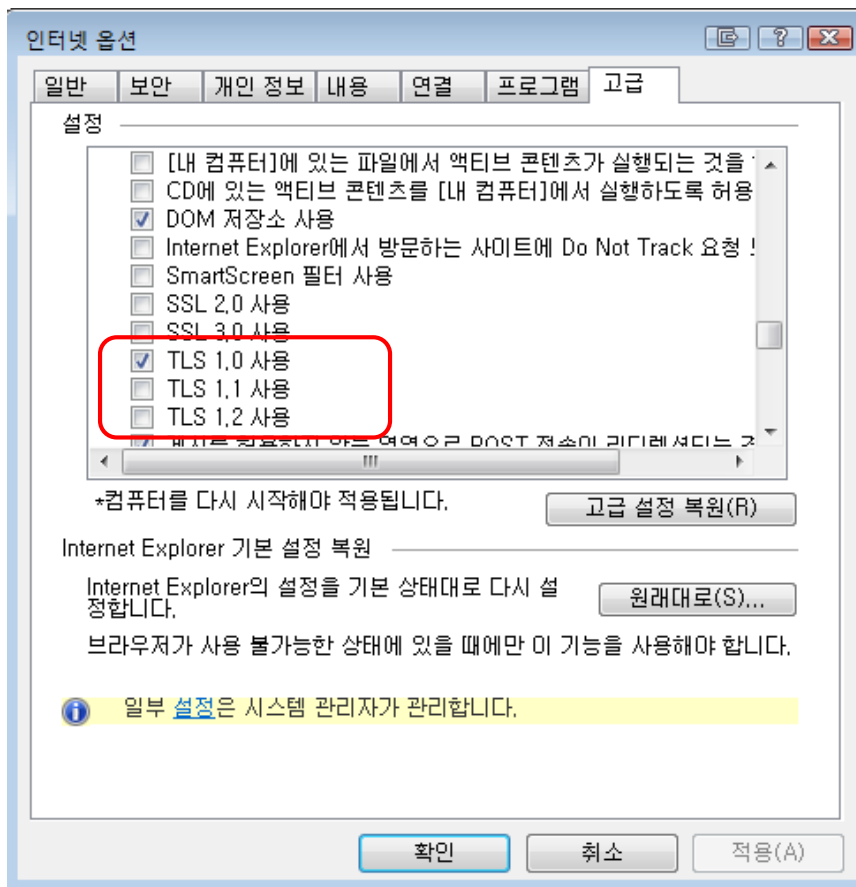
이 페이지를 표시할 수 없습니다.

[고급] 설정에서 TLS 1.0, TLS 1.1 및 TLS 1.2를 켜 다음 <https://dev.cnspay.co.kr:6464> 에 다시 연결해 보세요. 이 오류가 계속되는 경우 이 사이트는 지원되지 않는 프로토콜 또는 안전하지 않은 RC4 (세부 정보를 위한 링크)와 같은 암호 그룹을 사용할 수도 있습니다. 사이트 관리자에게 문의하세요.

설정 변경

2.2. 조치사항

- IE10 이하 버전에서는 보안 프로토콜 기본 설정 상태가 TLS1.1, TLS1.2 미사용 상태
- 조치사항 : 인터넷옵션 -> 고급 -> TLS1.1, TLS1.2 항목을 체크하여 사용 설정
- 최신 브라우저에서도 사용자가 강제로 옵션을 조정하였거나, 기타 다른 프로그램에 의하여 설정이 변경된 경우 오류 발생 가능



3. 영향 범위 및 조치사항 - 고객사(가맹점)

3.1. 영향 범위

- 고객사의 결제 서버가 상위 알고리즘을 지원하지 않는 서버인 경우 [고객사 <-> LG CNS] 서버 간 통신 불가 : 결제 오류 발생
- 따라서 아래의 [3.2. 조치사항] 과 같이 고객사(가맹점) 내 수정 및 적용 필요

3.2. 사용 언어 별 조치사항

- 다음과 같이 사용하는 언어 별 조치 내역 확인
- 고객사의 TLS 버전 확인 및 테스트 방법의 경우 [3.3.테스트 환경 제공 안내] 메뉴 참조

3.2.1. JAVA(JSP)

[Library 사용 시]

- JDK 1.6.0_111 버전 이상 사용 필수
➔ 위 버전 미만을 사용 할 경우 접속 불가 등의 현상이 발생 될 수 있음

[Restful API 사용 시]

- JDK 6, 7 버전은 아래와 같이 명시적으로 TLS 버전을 설정하는 코딩 추가 (JDK 1.6.0_111 미만 버전은 아래와 같이 설정해도 사용 불가)
- JDK 8 이상 버전은 Default 값이 TLS 1.2 이므로 별도 수정 없이 사용 가능
- JDK 1.6.0_111 이상 버전은 SSLContext.getInstance의 파라미터로 "TLS" 만 설정해도 사용 가능

```
public String sendHttps(String targetUrl, HttpServletRequest request,

    String sendData = "";
    String recvData = "";

    URL url = null;
    HttpURLConnection conn = null;

    try{
        url = new URL(targetUrl);
        conn = (HttpURLConnection)url.openConnection();

        SSLContext sc = SSLContext.getInstance("TLSv1.1");
        sc.init(null, null, new java.security.SecureRandom());
        conn.setSSLSocketFactory(sc.getSocketFactory());

        sendData = setSendParameters(request, hashValue, EncodeType);


        conn.setDoOutput(true);
        conn.setRequestMethod("POST");
        conn.setRequestProperty("Content-Type", "application/x-www-form-urlencoded");
        conn.setRequestProperty("Content-Length", Integer.toString(sendData.length()));
    } catch (Exception e) {
        e.printStackTrace();
    }

    return recvData;
}
```

3.2.2. PHP

- OS 내의 OpenSSL 버전 1.0.1e 이상 사용 필요
- 1.0.1e 미만인 경우 사용 불가

PHP Version 5.4.2



System	Linux localhost.localdomain 2.6.18-308.4.1.el5 #1 SMP Tue Apr 17 17:08:00 EDT 2012 x86_64
Build Date	Aug 2 2014 17:18:03
Configure Command	./configure '--prefix=/usr/local/php' '--with-mysql=/usr/local/mysql' '--with-apxs2=/usr/local/apache2/bin/apxs' '--disable-debug' '--with-iconv' '--with-gd' '--with-jpeg-dir' '--with-png-dir' '--with-libxml-dir' '--with-freetype-dir' '--with-zlib-dir' '--with-config-file-path=/usr/local/apache/conf' '--enable-sockets' '--with-openssl' '--with-mcrypt'

openssl

OpenSSL support	enabled
OpenSSL Library Version	OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008
OpenSSL Header Version	OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008

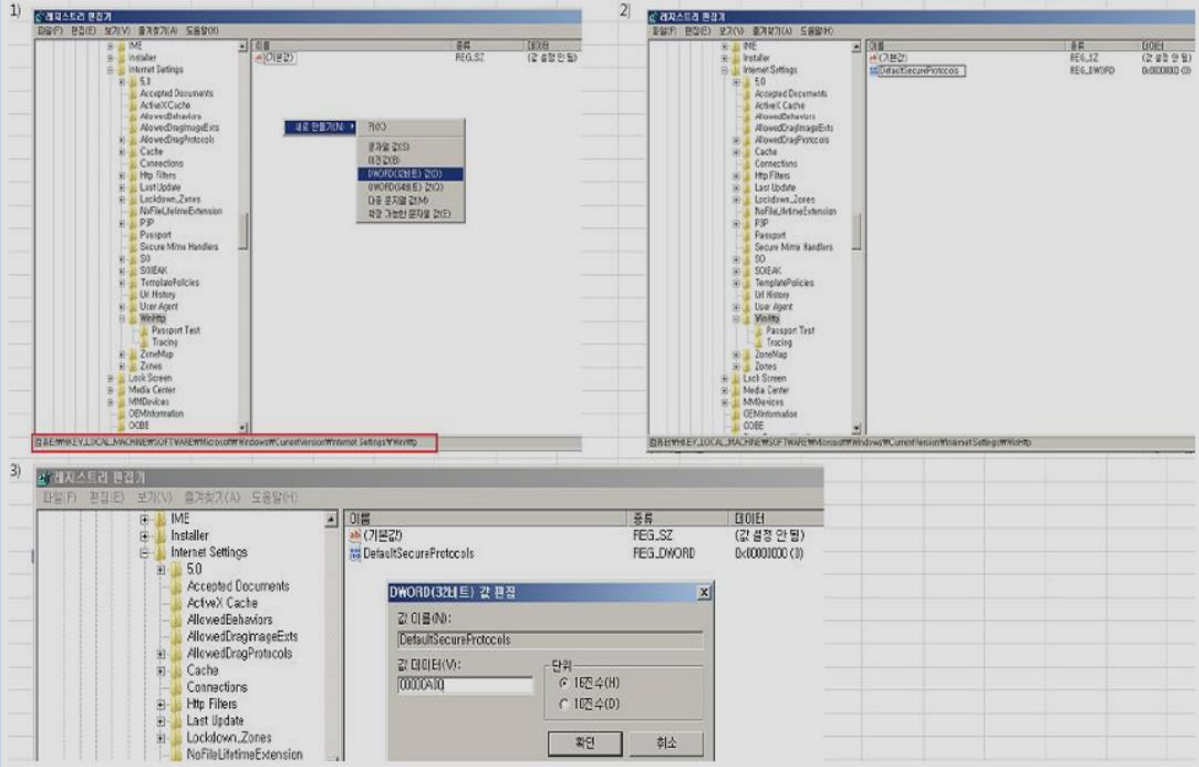
3.2.3. ASP

- Windows Server 2008 버전 이상 사용 필요
- 단, ASP "80072efd" 오류의 경우 아래와 같이 레지스트리 수정 처리 후 IIS 재부팅
- 32Bit Application 인 경우
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
➔ DefaultSecureProtocols=dword:00000A00
- 64Bit Application 인 경우
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
➔ DefaultSecureProtocols=dword:00000A00

1. 32 Bit Application 인 경우
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
DefaultSecureProtocols=dword:0000A00

2. 64 Bit Application 인 경우
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
DefaultSecureProtocols=dword:0000A00

수정 예시



3.2.4. ASP.NET (C#)

- Windows Server 2008 버전 이상 사용 필요
- 단, ASP.NET(C#) 오류 중 "원격측의 전송 스트림을 닫았으므로 인증에 실패했습니다." 인 경우 다음과 같이 코딩 추가 필요 (.NET Framework 4.5 이상)
- .NET Framework 4.0 사용 중 일 경우 아래 Tls11만 설정

```
30 String fdkTestUrl = "https://testicfs.firstdatacorp.co.kr/main.do"; //FDK TEST URL
31 String sendData = "test";
32 String rcvData = "";
33
34 TestUrl.Text = fdkTestUrl;
35
36 ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12;
37
38 //*****
39 // 4.URL 호출 처리
40 //*****
41 HttpWebRequest req = (HttpWebRequest)WebRequest.Create(fdkTestUrl);
42 req.Method = "POST";
43 req.ContentType = "application/x-www-form-urlencoded";
```


- TLS 1.1 적용을 위해 .NET Framework 버전을 아래와 같이 4.0 이상으로 적용 필요

.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

3.2.5. Python

- TLS 1.1 또는 TLS 1.2 를 지원하는 운영 체제에서 실행되는 경우 최신 버전과 호환
- Python 2.7.9 이상 : 기본적으로 TLS 1.1 이상과 호환
- Python 2.7.8 이하 : TLS 1.1 이상의 암호화를 지원하지 않음
- 즉, Python 2.7.9 이상 사용 필요

3.3. 테스트 환경 제공 안내

- 보안 취약 프로토콜 차단 이전 고객사에서 사용하는 TLS 버전을 확인 할 수 있도록 기존에 사용하는 결제 응답 값에 TLS 버전 파라미터를 신규 생성하여 고객사에 제공 (2019/04/11 부터 제공)

➔ 신규 파라미터 명 : TlsVer

- 위 파라미터의 값을 참조하여 사용중인 TLS 버전을 확인 할 수 있음
 - ➔ TLSv1 : TLS 1.0 버전
 - ➔ TLSv1.1 : TLS 1.1 버전
 - ➔ TLSv1.2 : TLS 1.2 버전
- 승인 및 취소, TID 상태조회 등 고객사의 요청에 대한 응답 Transaction에 위 TLS버전 확인을 위한 신규파라미터가 전달되므로 해당 값을 참고하여 TLS 1.0 이하 버전을 사용 할 경우 TLS 업그레이드 적용 필요
- 고객사에서 각 트랜잭션마다 다른 환경에서 호출하는 경우가 있으므로 (예를들면 승인과 취소를 다른 서버환경에서 요청하여 환경 별로 사용하는 TLS 버전이 상이) 사용하시는 모든 트랜잭션에 대해 테스트 필요

4. FAQ

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

A. IE 10 이하 브라우저의 경우에 해당됩니다. (‘2. 영향 범위 및 조치사항 - 결제 고객’ 확인)
IE 브라우저 설정 변경을 통해 사용 가능합니다.

Q. 신 IE 브라우저의 경우에도 결제창 호출이 되지 않는 경우가 있나요?

A. 사용자가 강제로 브라우저의 옵션을 조정하였거나 기타 프로그램들에 의해 인터넷 설정이 TLS 미사용

또는 TLS 하위버전만 사용하게 변경 된 경우 결제창이 뜨지 않고 “이 페이지를 표시할 수 없습니다.” 라는 화면이 노출될 수 있습니다.

사용자의 브라우저에서 '인터넷옵션-고급-TLS1.1, 1.2 사용 설정해야 합니다.

Q. 고객사(가맹점) 에서 조치해야 할 사항이 있나요?

A. 고객사의 결제 서버가 상위 프로토콜/알고리즘을 지원하지 않는 경우 결제 요청을 위한 통신이 불가능 하며 언어에 따라 고객사 서버에서 소스 수정 또는 서버 환경 설정이 필요합니다.

(결제 승인 시 고객사 서버 => LG CNS 서버 간 통신 불가)

Q. 정확히 언제부터 적용되나요?

A. 보안 취약 프로토콜 차단 작업을 2019년 7월 1일 월요일에 진행 예정입니다. 따라서 고객사에서는 2019년 6월 30일 일요일까지 TLS 1.1 이상을 사용하도록 적용 해 주셔야 합니다.

현재 고객사에서 사용하는 TLS버전의 경우 [3.3.테스트 환경 제공 안내] 메뉴를 참고하셔서 확인하시기 바랍니다.

Q. 기술 관련 사항으로 문의 할 점이 있습니다. 어디로 연락하면 되나요?

A. 아래의 LG CNS 기술지원 담당에게 문의 주시면 됩니다.

tech.cnspay@lqcns.com / 02-2099-2385