< OpenSSL Drown 취약점 대응 FAQ >

OpenSSL Drown 취약점 대응 FAQ

Q1. 시스템에서 OpenSSL의 버전 정보를 어떻게 확인할 수 있나요?

○ 대상 시스템의 터미널에 접속하셔서 아래의 명령어를 입력하여 버전을 확인하실 수 있습니다.

- **명령어를 통한 OpenSSL 버전 정보 확인**

root@server:~# **openssl version**

OpenSSL 1.0.1f 6 Jan 2014

Q2. 보안 패치가 정상적으로 설치가 되었는지 어떻게 확인할 수 있나요?

○ 터미널에 접속한 후 아래의 명령어를 실행하여 1.0.2g나 1.0.1s 이라는 메시지가 출력되면 보안 패치가 완료된 것입니다.

- 아래 명시한 최신 업데이트 버전은 OpenSSL에서 공식적으로 배포한 버전으로 각 OS벤더(ubuntu, redhat, centos 등)별로 최신 버전 관리 체계가 상이할 수 있으니 참고하시기 바랍니다.

openssl version

OpenSSL 1.0.2g 1 Mar 2016

openssl version

OpenSSL 1.0.1s 1 Mar 2016

Q3. 보안 패치를 적용한 후 서버 재부팅이 필요하나요?

○ 업데이트 후 모든 서비스에 적용하기 위해서 해당 관련 서비스의 재시작을 권장 드립니다.

Q4. 소스코드 형태로 된 보안 패치 파일은 어디에서 받아 볼 수 있나요?

○ OpenSSL 공식 사이트에 방문하여 최신 패치 파일을 다운로드 받아 설치할 수 있습니다.

- **다운로드 링크 : ftp://ftp.openssl.org/source/**

Q8. apt-get 또는 yum을 이용한 자동 업데이트가 되지 않을 경우 어떻게 해야 하나요?

○ apt-get, yum을 통한 자동 업데이트는 인터넷에 연결하여 업데이트 파일을 받아오기 때문에 먼저 업데이트 대상 서버가 인터넷에 연결되어 있는지 확인하신 후 업데이트를 적용하시기 바랍니다.

○ 인터넷에 연결되지 않은 서버의 경우 rpm 등의 패키지를 다운받을 수 있는 사이트에 접속하여 패치 파일을 다운로드하여 로컬 시스템에 설치할 수 있습니다. (Q9 참고)

Q9. 인터넷이 되지 않는 내부에서 운영하는 서버는 어떻게 보안 패치를 수행할 수 있나요?

○ 업데이트 대상 시스템이 인터넷에 연결되어 있지 않아 apt-get, yum을 통한 자동 업데이트를 수행할 수 없을 경우 OpenSSL의 최신 패치 파일을 별도의 인터넷이 연결된 곳에서 다운로드 한 후 로컬 시스템에 업로드하여 수동으로 보안 패치를 적용할 수 있습니다.

○ OpenSSL 최신패치 다운로드 사이트

- ftp://ftp.openssl.org/source/

Q. 수동 업데이트 하는 방법이 있나요?

○ 수동 업데이트 설치 방법

(예제)

1. # wget http://www.openssl.org/source/최신버전
2. # tar –zxf openssl-1.0.1s.tar.gz
3. # cd openssl.1.0.1s
4. # ./config —prefix=/usr —openssldir=/usr/local/openssl shared
5. # make
6. # make install
7. # openssl version

Q. 지금 현재 취약점은 몇 개이며 왜 발생하였나요?

○ 아래와 같이 현재 발생한 취약점은 총 8개이며, 설명은 아래와 같습니다.

CVE 번호	출현 날짜	취약점	요약
CVE-2016-8000	2014-09-24	정보 유출	SSLv2를 지원하는 서버의 암호화된 TLS 통신 데이터를 복호화할 수 있는 취약점
CVE-2016-0705	2014-09-24	서비스 거부	특수하게 조작된 DSA 개인키를 처리하는 과정에서 메모리 충돌이 발생하여 서버에 서비스 거부 공격이 가능한 취약점
CVE-2016-0798	2014-09-25	메모리 누출	SRP를 운영하는 서버에 특수하게 조작된 패킷을 전송할 경우, 서버의 메모리 정보가 누출될 수 있는 취약점
CVE-2016-0797	2014-09-26	서비스 거부	BN_hex2bn 함수에서 데이터를 변환하는 과정에서 메모리 충돌이 발생할 수 있는 취약점
CVE-2016-0799	2014-09-27	임의코드 실행	BIO_printf 함수에서 데이터를 처리하는 과정에서 발생하는 오버플로우 취약점
CVE-2016-0702	2014-09-29	정보 유출	cache-bank conflict를 이용한 부채널 공격으로, RSA 키를 복구할 수 있는 취약점
CVE-2016-0703	2014-09-29	정보 유출	평문 일부를 알고 있을 때, 암호화된 다른 부분을 복호화 할 수 있는 취약점
CVE-2016-0704	2014-09-29	정보 유출	Bleichenbacher를 통해 암호문을 보호한 경우, 잘못된 바이트로 마스터키를 덮어쓸 수 있는 취약점

Q. 윈도우 서버를 사용 중인데 패치해야 하나요?

○ 윈도우 서버의 경우 IIS/NSS 및 Apache윈도우 버전을 사용 중이면 SSLv2을 사용안함으로 설정해야 합니다.

- Microsoft IIS SSLv2 사용안함 설정

1. "시작"을 클릭하고 "실행"을 클릭한 다음, regedt32 혹은 regedit을 타이핑한 후 "확인"을 클릭
2. 레지스트리 편집기에서 다음 레지스트리 키로 이동한다

HKey_Local_Machine₩System₩CurrentControlSet₩Control₩SecurityProviders₩SCHANNEL₩Protocols₩SS2.0₩Server

3. 편집 메뉴에서 "값 추가"를 클릭한다.
4. "데이터 형식" 목록에서 DWORD를 클릭한다.
5. "값 이름" 박스에 "Enabled"를 타이핑하고 "확인"을 클릭한다.
6. 새로운 키의 값을 "0"으로 설정하기 위해 이진 편집기에 00000000을 타이핑한다.
7. "확인"을 클릭하고 IIS를 재시작한다.

Q. 현재 버전이 0.9.8 또는 0.9.7 버전을 사용 중 인데, 패치를 해야 하나요?

○ 현재 0.9.7 버전은 OpenSSL에 지원이 종료된 상태이고, 0.9.8 및 1.0.0 버전 또한 2015년 12월 31일부로 서비스가 종료되었으므로, 해당 버전을 사용 중이면 1.0.2g 또는 1.0.1s 버전으로 업데이트를 권고 드립니다.