2014 Security Issue : Heart Bleed / Shell Shock

Lim, JeWon

Who am I?

- JTJSoft Member
- SecurityPlus Student Academy
- Best of the Best 4th Member

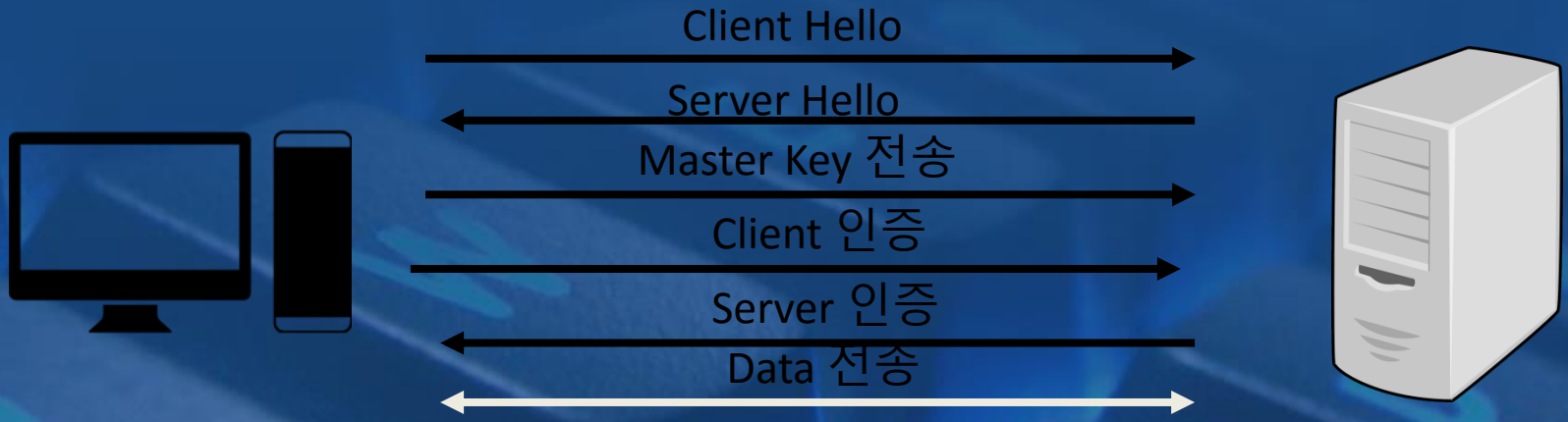
오늘 발표할 내용이란..

Shellshock

Heart Bleed 취약점에 대해 알아보기 전에...

What is **OpenSSL**?

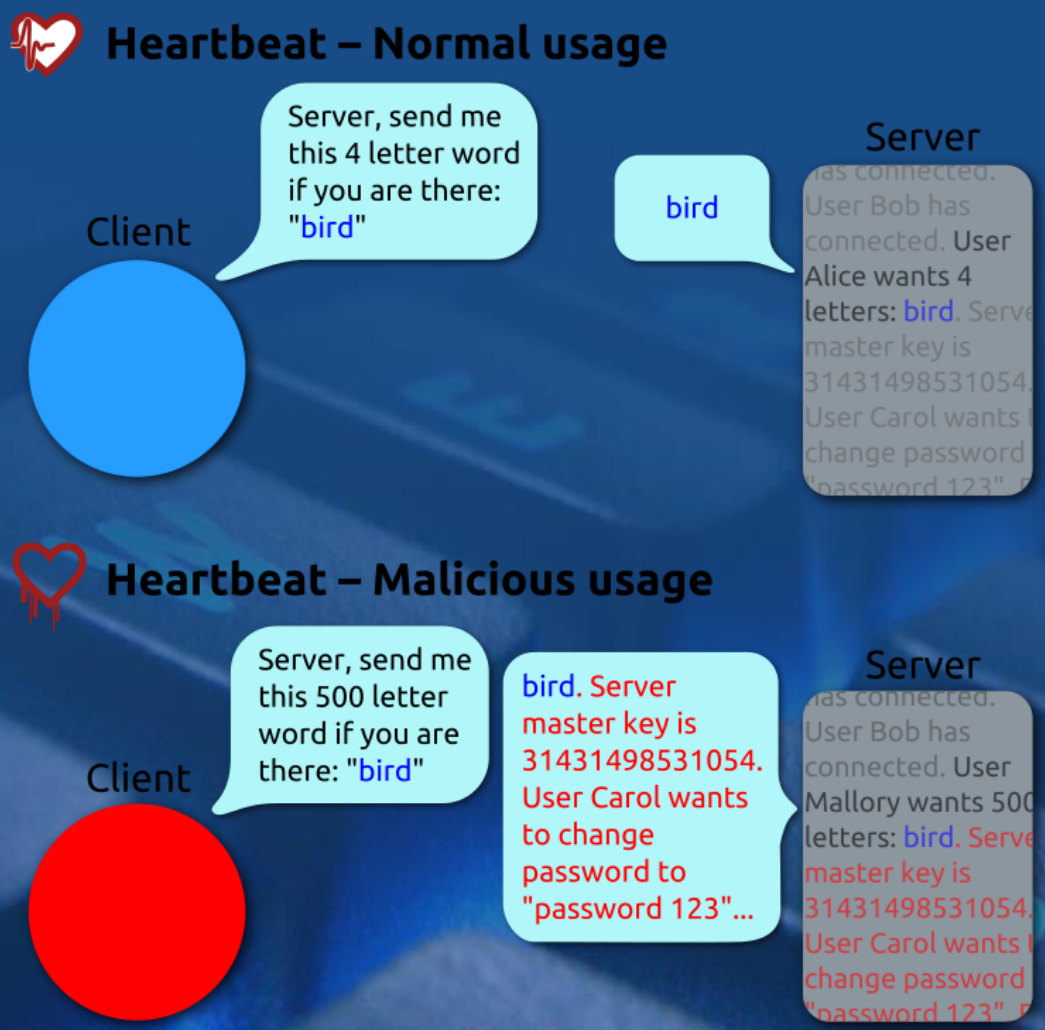
- **SSL** : 웹 서버와 브라우저 사이의 보안을 위해 만들어진 프로토콜. (https://)



What is **OpenSSL**?

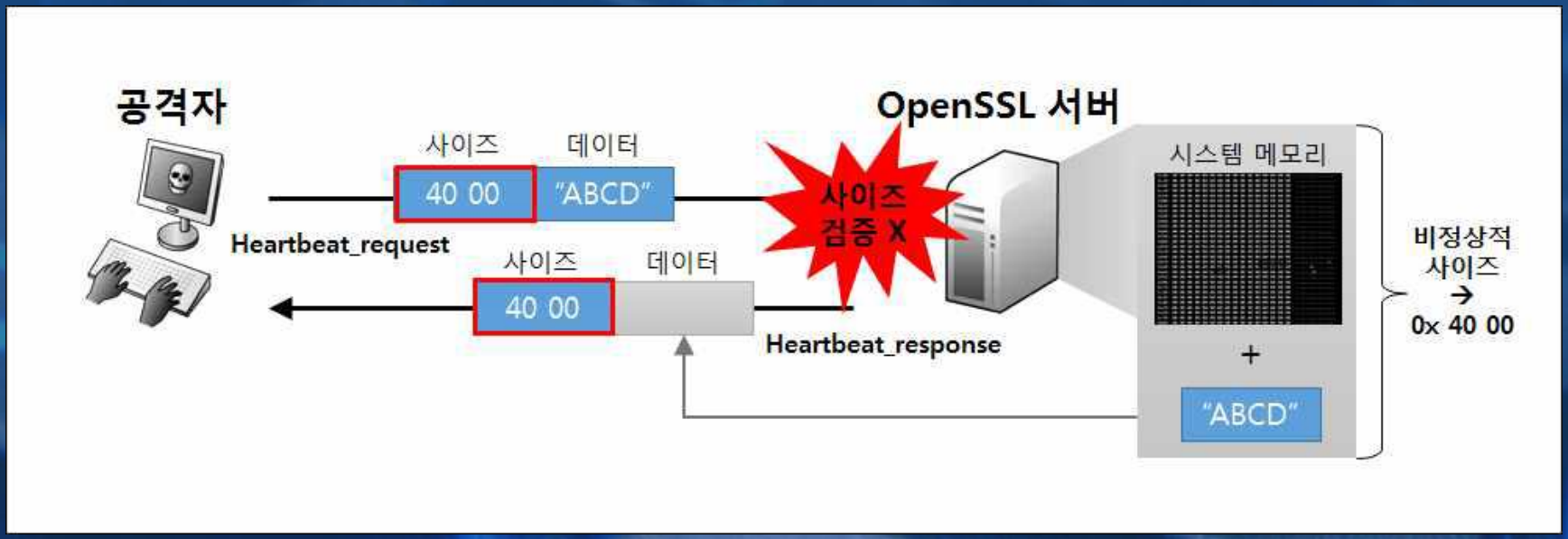
- OpenSSL : 앞에서 설명한 SSL의 오픈소스 구현판.

Heart Bleed


Heartbeat – Normal usage
Server, send me this 4 letter word if you are there: "bird"
Client
bird
Server
has connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". E
Heartbeat – Malicious usage
Server, send me this 500 letter word if you are there: "bird"
Client
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
has connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". E

공격 방법

- HeartBeat Request 패킷의 메시지 길이 정보를 변조하여 취약한 OpenSSL을 사용중인 서버에 전송.



취약점 여부 확인(1)

- http://filippo.io/Heartbleed/

취약점 여부 확인(2)

- OpenSSL버전 확인
- Openssl version –a 쳐서
- OpenSSL 1.0.1 ~ OpenSSL 1.0.1f
- OpenSSL 1.0.2-beta, OpenSSL 1.0.2-beta1
- 로 나오면 업데이트 요망.

취약점 여부 확인(3)

- HeartBeat 활성화 여부 확인

- **openssl s_client –connect domain.com:443 –tlsextdebug –debug –state | grep -i heartbeat**

- **취약 버전이 HeartBeat를 사용하지 않으면 취약점의 영향력에 포함되지 않음.**

취약점 여부 확인(4)

```
if (1 + 2 + 16 > s -> s3 -> rrec_length)          // patch!
    return 0;

hbtype = *p++;

n2s(p, payload);

if(1 + 2 + payload + 16 > s -> s3 -> rrec.length) // patch!
    return 0;

pl = p;
```

Heart Bleed Attack script

- http://www.exploit-db.com/exploits/32745/
- https://github.com/sensepost/heartbleed-poc/blob/master/heartbleed-poc.py
- https://raw.githubusercontent.com/musalbas/heartbleed-masstest/master/ssltest.py
- http://nmap.org/nsedoc/scripts/ssl-heartbleed.html
- http://www.exploit-db.com/exploits/32791/

대응방안(개인 사용자)

- 업데이트

- apt-get update
- yum update

대응방안(네트워크 장비)

- Snort 를 이용한 취약점 공격 탐지 및 차단 패턴 적용

대응방안(시스템 관리)

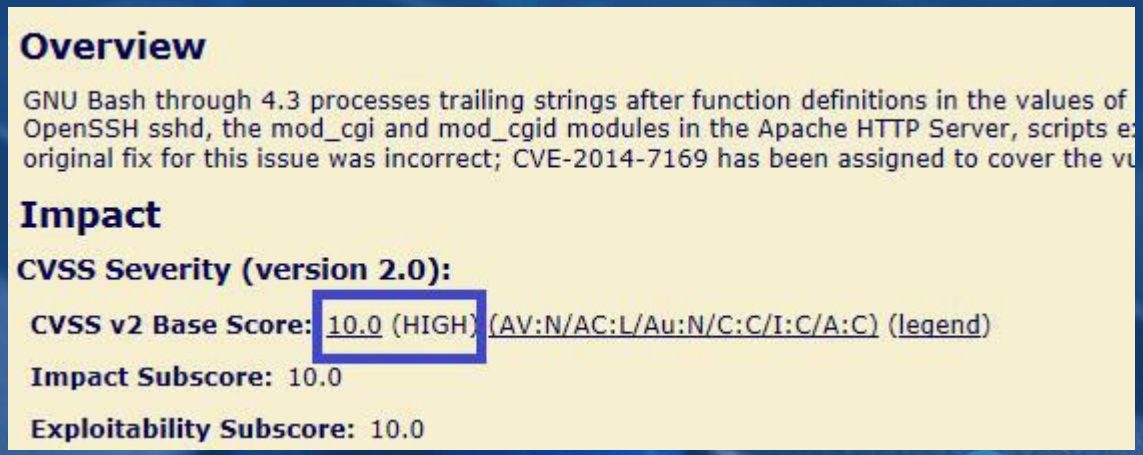
- 인증서 재발급 검토
- 유저들의 비밀번호 재설정 유도

반응

- 브루스 슈나이어 : 보안 위협 점수를 1부터 10까지 매긴다면 Heart Bleed는 11이다.
- Kaspersky lab : Open SSL에 의존 하던 많은 웹사이트들에서 얼마나 정보가 빠져나갔는지 추정이 불가능하다.
- 금융권 : (충격과 공포)
- 한국 : Open SSL이 뭐죠?

Shell Shock

- Bash 쉘 에서 나온 취약점으로 Heart Bleed 보다 더 광범위한 영향력을 끼친 취약점.



Overview

GNU Bash through 4.3 processes trailing strings after function definitions in the values of
OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts e
original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vu

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

Shell shock Test

- **$ env x='() { :;}; echo UbuntuK' bash -c "echo Ubuntu Korea“**

- 이걸 쳐서 아웃풋이

  UbuntuK

  Ubuntu Korea

  로 나오면 당신은 망한 겁니다.

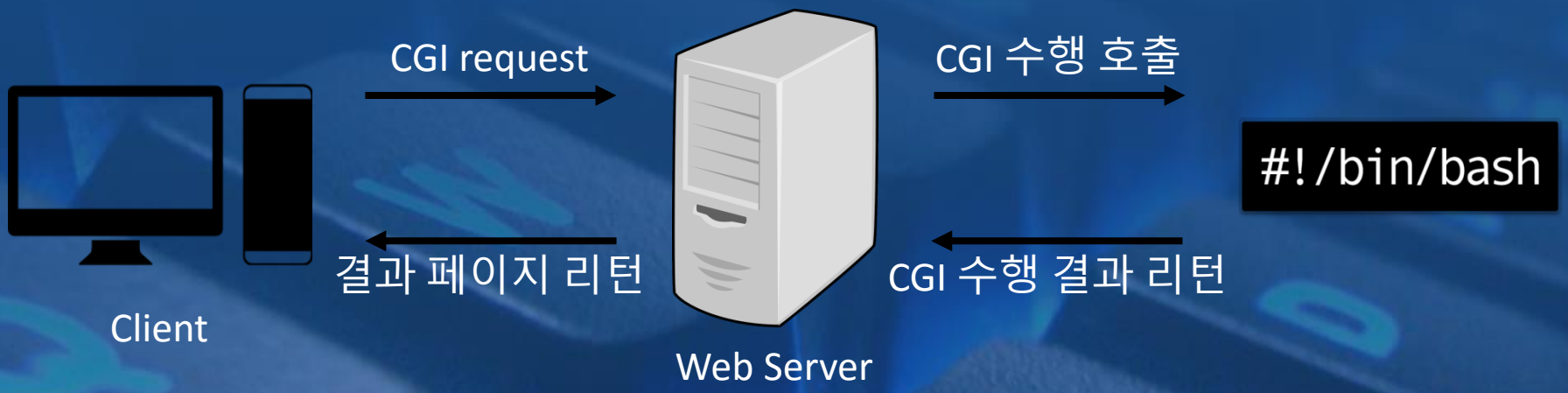
(근데 요즘 배포판은 전부 패치 해서 안전할 거임. 아마 ㅎㅎ)

Shell Shock 취약점

번호	취약점
CVE – 2014 – 6271	원격 명령 실행
CVE – 2014 – 7169	함수 선언문 파싱 에러
CVE – 2014 – 7186	잘못된 메모리 접근
CVE – 2014 – 7187	잘못된 메모리 접근
CVE – 2014 – 6277	함수 선언문 파싱 에러
CVE – 2014 – 6278	원격 명령 실행

콘솔 접속(SSH)만 차단하면 되는 거 아님?

- 콘솔 환경이 아니더라도 bash 수행이 가능한 환경들이 있다. (이를테면 'CGI')

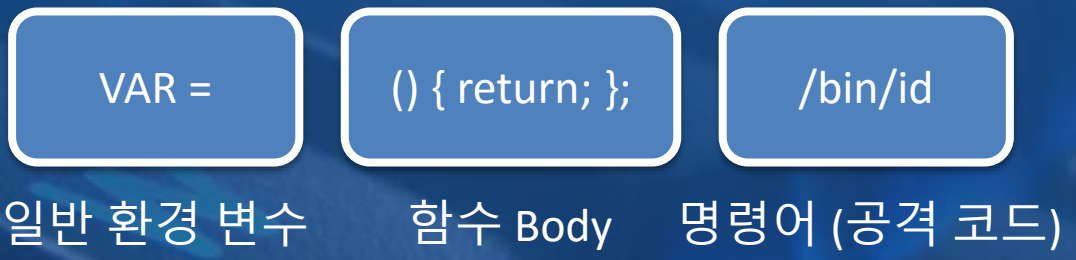


취약한 프로그램은 더 있다.

- NAS
- OpenVPN
- DHCP
- Nginx
- Qmail
- Etc.

GNU Bash

발생 원인 분석



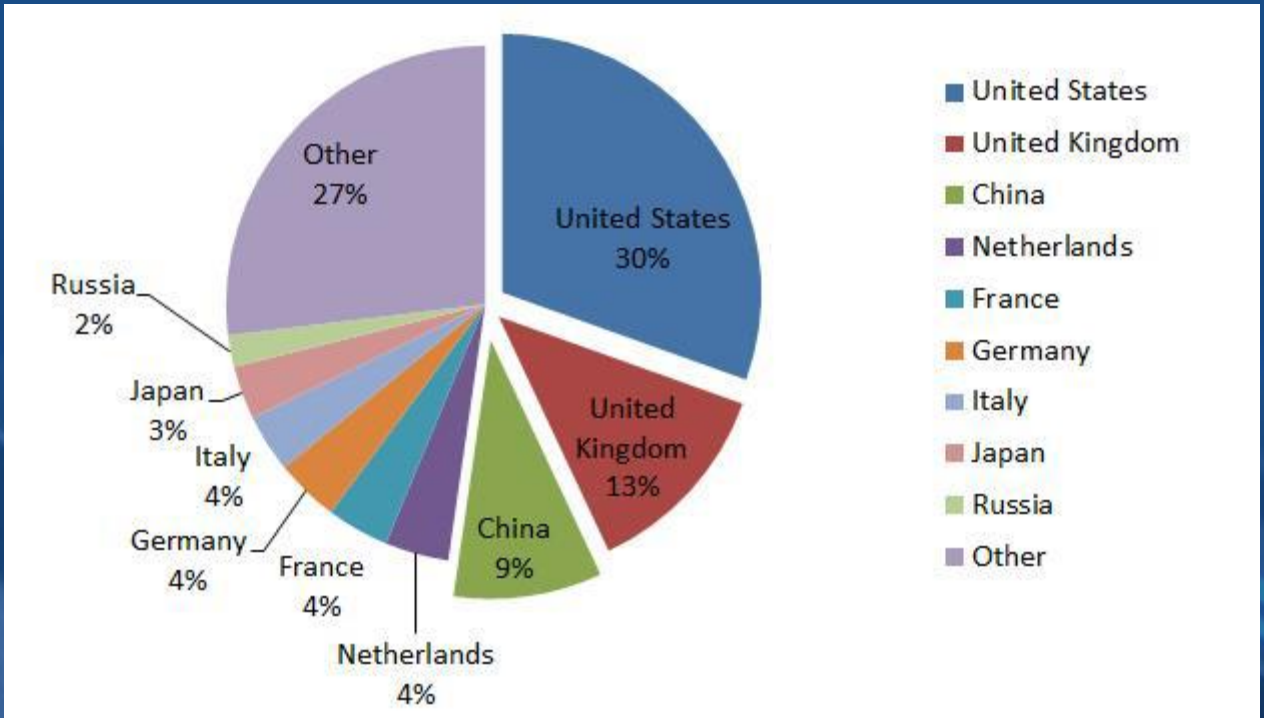
소스코드 분석

- Shell Shock발생 원인을 알아보기 위해서는 Bash의 evalstring.c 소스를 분석해볼 필요가 있다.

```
int parse_and_execute(string, from_file, flags)
{
    ...

    while(*(bash_input.location.string))
    {
        ...
    }
}
```

공격 동향


Other
27%
United States
30%
United
Kingdom
13%
China
9%
Netherlands
4%
France
4%
Germany
4%
Italy
4%
Japan
3%
Russia
2%
United States
United Kingdom
China
Netherlands
France
Germany
Italy
Japan
Russia
Other

대응방안(1)

- Bash update

대응방안(2)

- 사용하지 않는 CGI 페이지 서비스 중지

대응방안(3)

- Snort 를 이용한 취약점 공격 탐지 및 차단 패턴 적용

교훈

- Heart Bleed / Shell Shock 사태는 오픈소스에 대한 관심과 사랑의 부족을 말해주고 있다!