OpenSSL 漏洞檢測與安全性修補

財團法人國家實驗研究院

國家高速網路與計算中心

目錄

一、SSL 網路傳輸加密協定

SSL(Secure Socket Layer)是一種應用廣泛的網路加密傳輸協定，透過公開金鑰(Public Key)的技術，SSL 可以對網路傳輸內容加密，以確保資料的機密性與完整性，免於遭到竊聽或是竄改。SSL 目前是最常被使用的網路傳輸安全協定，一般網站用來確保用戶傳輸資料安全的 HTTPS(Hypertext Transfer Protocol Secure)傳輸協定，即屬於 SSL 的應用。

二、Open SSL 的安全性漏洞

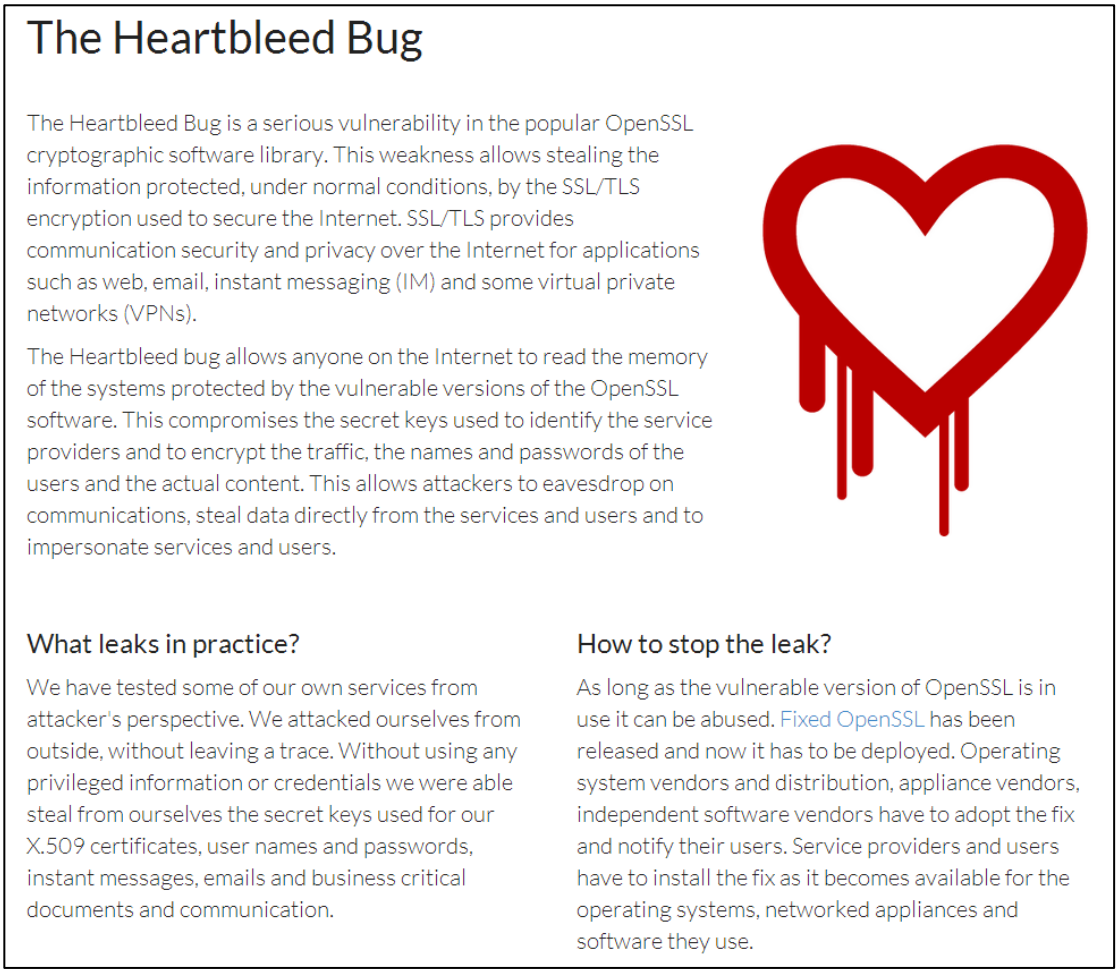
OpenSSL 是基於 SSL 所發展的開放原始碼(Open Source)的安全協定，也是目前最常被使用的 SSL 應用。日前 Google 資安人員 Neel Mehta 發現 OpenSSL 1.0.1 版的 HeartBeet 擴充功能存在嚴重的安全性漏洞，可以讓遠端攻擊者存取記憶體中未經保護的資料。該資訊公開後，OpneSSL 隨即緊急進行漏洞修補並發出告警訊息，而 CVE(Common Vulnerability and Exposures)漏洞資料庫也將其正式列為 CVE-2014-0160。雖然 Open SSL 0.9.8 版不受 Heartbleed bug 影響，但 0.9.8 版仍然存在多項已知的安全性漏洞，建議系統管理員須注意其安全性更新狀態。

CVE-2014-0160 的漏洞敘述如下：

CVE 編號	CVE-2014-0160
說明	OpenSSL 1.0.1g 之前的版本，未能正確地處理 HeartBeet 擴充模組的封包，導致遠端攻擊者可以利用這個漏洞取得記憶體中的敏感資訊，例如私鑰(private key)。 The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
漏洞敘述	TLS 的 heatbeet 擴充套件存在系統漏洞，攻擊者可以利用這個漏洞存取正在連線的伺服器端或是用戶端的記憶體內 64K 的敏感資訊， A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server.
影響系統	包含 Open SSL 1.0.1f 版與 OpenSSL 1.0.2-beta 版之前的所有版本會受到影響。 Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including 1.0.1f and 1.0.2-beta1.

三、OpenSSL Heartbleed 漏洞檢測

OpenSSL 的應用廣泛，舉凡 https 網頁瀏覽、SSH 安全連線、SSL VPN 虛擬私有網路等，都有可能使用 OpenSSL 來進行內容加密，受影響的設備除了網頁伺服器、應用程式伺服器外，網路通信設備與手持終端設備亦有可能會受到影響。因此，建議系統與網路管理員可以透過以下幾種方式進行自我檢測，以確認設備或服務是否受到 Heartbleed 的漏洞影響。



The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

What leaks in practice?

We have tested some of our own services from attacker's perspective. We attacked ourselves from outside, without leaving a trace. Without using any privileged information or credentials we were able steal from ourselves the secret keys used for our X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication.

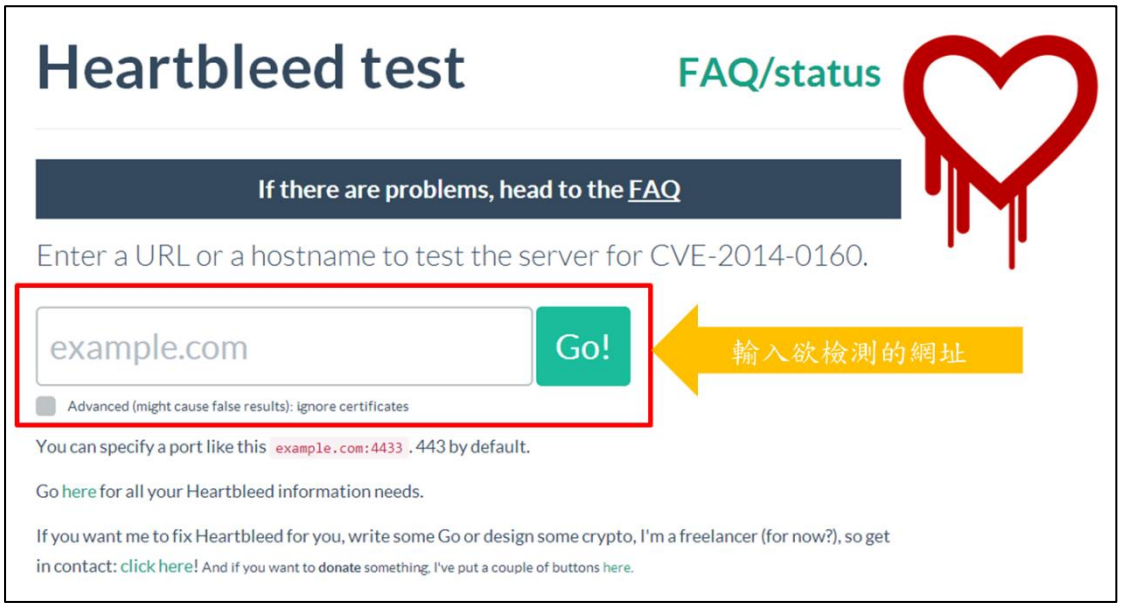
How to stop the leak?

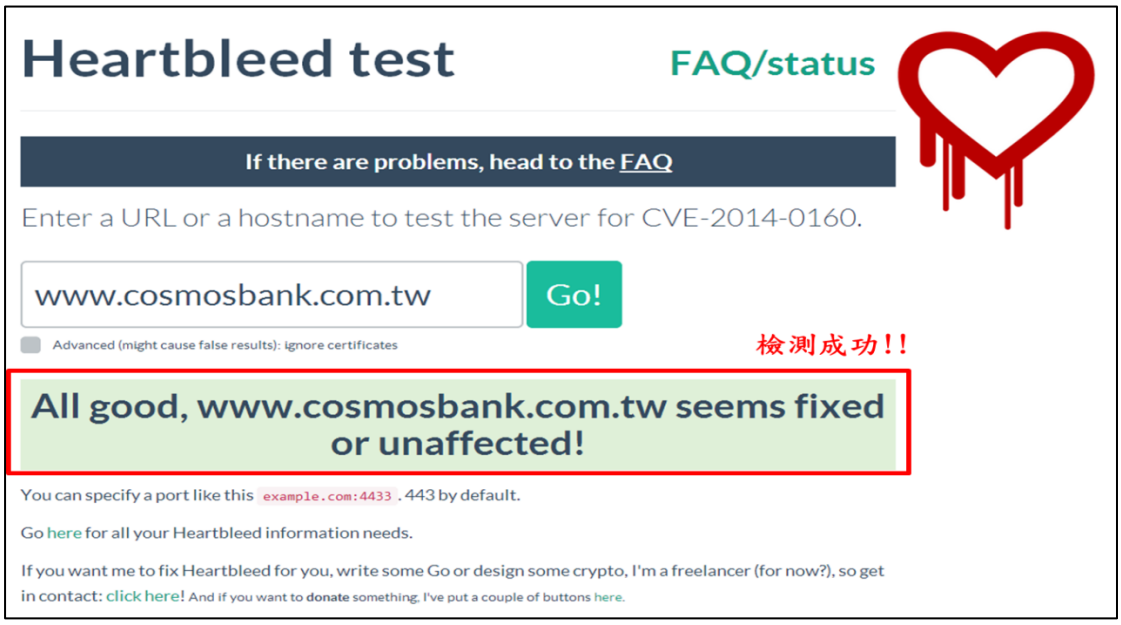
As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been released and now it has to be deployed. Operating system vendors and distribution, appliance vendors, independent software vendors have to adopt the fix and notify their users. Service providers and users have to install the fix as it becomes available for the operating systems, networked appliances and software they use.

(一) 線上檢測

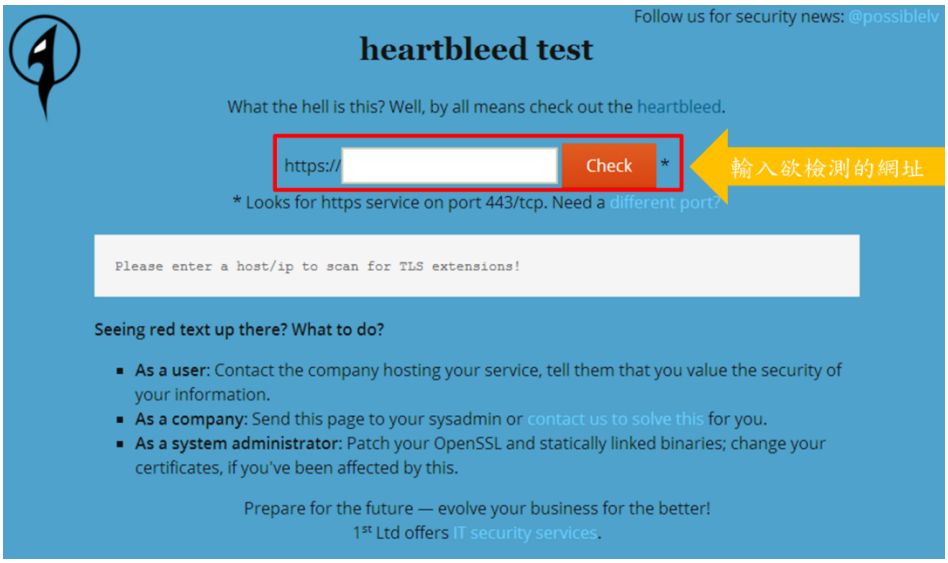
目前網路上有兩個公開檢測網站，使用者僅需要輸入目標網站網址，就可以進行 Heartbleed 的漏洞檢測：

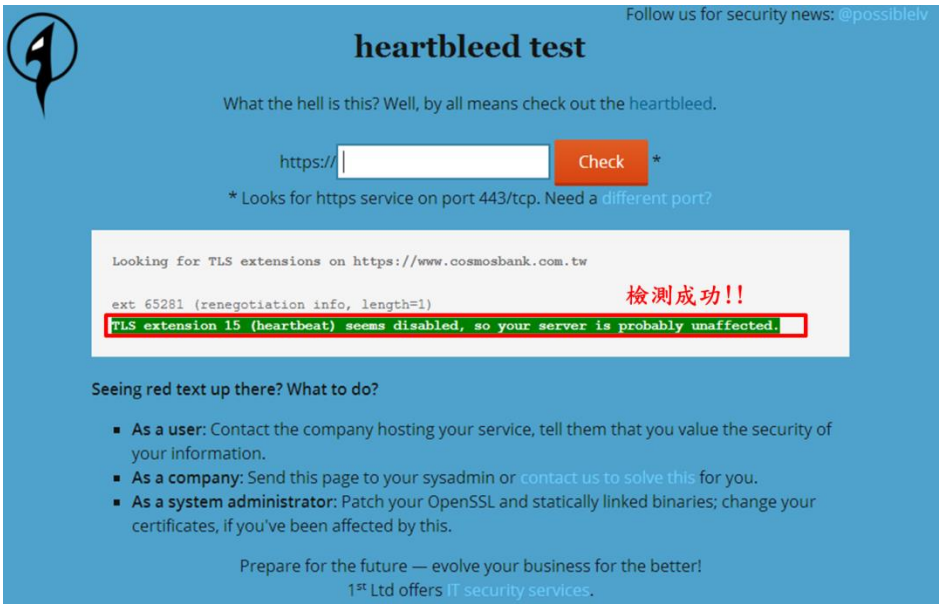
1. https://filippo.io/Heartbleed/





2. http://possible.lv/tools/hb/





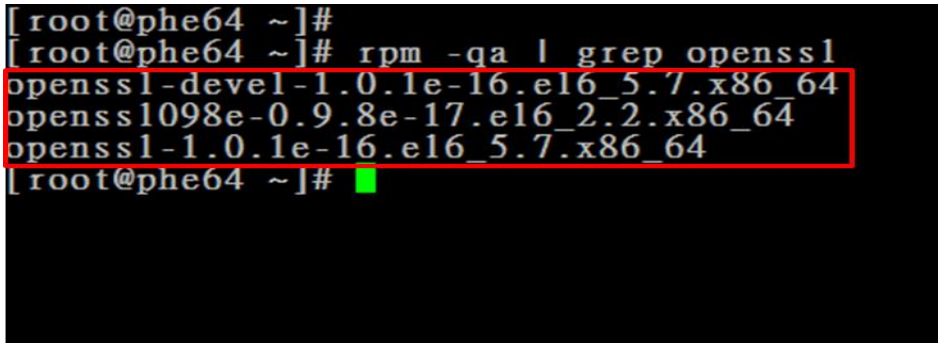
（二） 自我檢測

系統管理員可以登入伺服器，透過套件檢索的方式，直接進行 OpenSSL 的套件版本檢查，以下就常見的 redhat 與 debian 系統進行說明：

1. Redhat 系統(以 Scientific Linux 6.5 為例)

管理員可以藉由輸入以下指令，來搜尋主機中已經安裝的 OpenSSL 套件，並確認其版本：

```
#rpm -qa | grep openssl
```



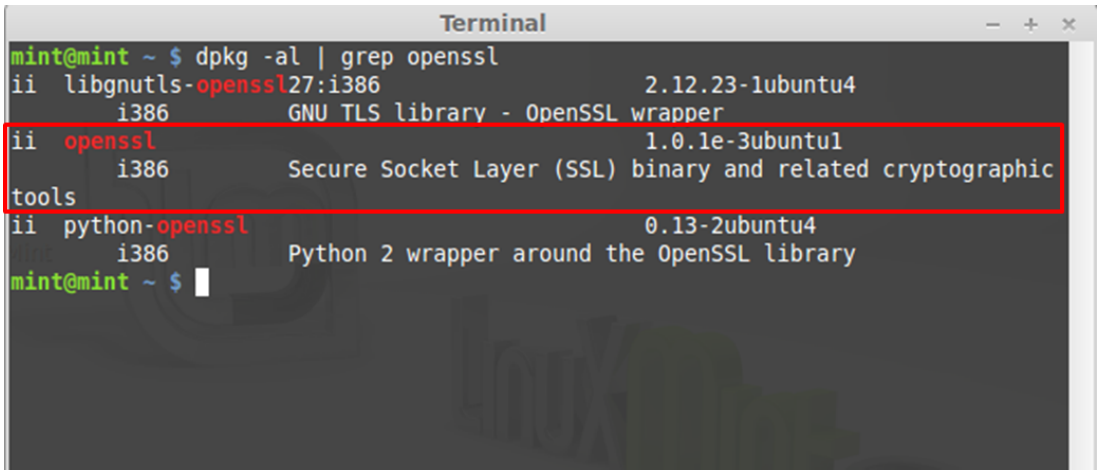
檢測結果顯示,該主機之 OpenSSL 套件為 1.0.1e-16.el6_5.7 版，根據 Redhat 官網所公佈之安全性更新說明，已經修正 OpenSSL 的安全性問題，不會受到此次 HeartBleed Bug 的影響。

- RedHat 官方說明請參考以下網址：
  https://rhn.redhat.com/errata/RHSA-2014-0376.html
- CentOS 官方說明請參考以下網址：
  http://www.centosblog.com/critical-openssl-vulnerability-heartbleed-openssl-1-0-1-1-0-1f-patch-bug-centos-system/

2. Debian 系統(以 Linux Mint 16 系統為例)

管理員可以藉由輸入以下指令，來搜尋主機中已經安裝的 OpenSSL 套件，並確認其版本：

```
~ $ dpkg -al | grep openssl
```



檢測結果顯示，該主機之 OpenSSL 套件版本為 1.0.1e-3ubuntu1，會受到此次 HeartBleed Bug 的影響，可能存在資安威脅，建議管理員儘早 將 OpenSSL 的套件升級至 1.0.1e-3ubuntu1.2。

- Debian 的說明請參考以下網址：

  https://security-tracker.debian.org/tracker/CVE-2014-0160

- Ubuntu 的官方說明請參考以下網址：

  http://www.ubuntu.com/usn/usn-2165-1/

四、OpenSSL Heartbleed 安全性修補

(一)系統更新

1. Redhat 系統

管理員可以輸入以下指令，來指定 OpenSSL 模組進行更新，升級結束後請記得重新啟動相關應用服務：

```
#yum update openssl
```

2. Debian 系統

管理員可以輸入以下指令，來指定 OpenSSL 模組進行更新，升級結束後請記得重新啟動相關應用服務：

```
#sudo apt-get install --only-upgrade openssl
```

(二)其他設備

因 OpenSSL 應用廣泛，部份網路通信設備或資安設備也使用 OpenSSL 作為其通訊加密協定。因此，若管理員無法自行操作 OpenSSL 的版本檢查與更新，請向原廠工程師諮詢並尋求相關技術支援。

可能受到 OpenSSL 影響的網路通信設備如下：

製造商	是否受到 OpenSSL Heartbleed Bug 影響	參考網址
A10	不受影響	https://www.a10networks.com/vadc/index.php/a10-products-not-vulnerable-to-openssl-cve-2014-0160-heartbleed/
Aruba Networks	部份產品	http://www.arubanetworks.com/support/alerts/aid-040814.asc
BlueCoat	部份產品	https://kb.bluecoat.com/index?page=content&id=SA79&actp=LIST
CheckPoint	部份產品	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk100173
Cisco	部份產品	https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk100173
Extreme Networks	部份產品	https://esupport.extremenetworks.com/
F5	部份產品	http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15159.html
FireEye	部份產品	http://www.fireeye.com/resources/pdfs/support-notices/fireeye-statement-about-openssl-heartbleed-vulnerability-cve-2014-0160.pdf
Fortinet	部份產品	http://www.fortiguard.com/advisory/FG-IR-14-011/
iMPERVA	部份產品	http://www.imperva.com/resources/adc/adc_advisories_response_heartbleed_CVE-2014-0160.html
Juniper	部份產品	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623&actp=SUBSCRIPTION
Palo Alto	不受影響	http://researchcenter.paloaltonetworks.com/2014/04/palo-alto-networks-addresses-heartbleed-vulnerability-cve-2014-0160/
Ruckus	部份產品	http://www.ruckuswireless.com/security
Sophers	部份產品	http://blogs.sophos.com/2014/04/08/important-note-openssl-vulnerability-cve-2014-0160-in-sophos-utm/
Splunk	部份產品	http://www.splunk.com/view/SP-CAAAMB3

TippingPoint	不受影響	https://tmc.tippingpoint.com/TMC/library/announcements/heartbleed_openssl_vulnerability.pdf
VMware	部份產品	http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2076225
Websense	部份產品	http://www.websense.com/support/article/kbarticle/Heartbleed-OpenSSL-Vulnerability

(四)參考資料

1. OpenSSL Security Advisoty, https://www.openssl.org/news/secadv_20140407.txt
2. CVE-2014-0160, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
3. http://en.wikipedia.org/wiki/Transport_Layer_Security#BEAST_attack
4. Heartbleed test, https://filippo.io/Heartbleed/
5. heartbleed test, http://possible.lv/tools/hb/
6. OpenSSL Heartbleed 全球駭客的殺戮祭典，你參與了嗎？, http://devco.re/blog/2014/04/11/openssl-heartbleed-how-to-hack-how-to-protect/
7. https://rhn.redhat.com/errata/RHSA-2014-0376.html
8. http://www.centosblog.com/critical-openssl-vulnerability-heartbleed-openssl-1-0-1-1-0-1f-patch-bug-centos-system/
9. https://security-tracker.debian.org/tracker/CVE-2014-0160
10. http://www.ubuntu.com/usn/usn-2165-1/
11. http://jal.tw/cve:cve-2014-0160