Mail2000 v6
安全性程式更新手冊

網擎資訊軟體股份有限公司 謹呈
Openfind Information Technology, Inc.

2014.04.10

前言

OpenSSL 是一個開放源碼網路傳輸加密函式庫，使用相當廣泛，Apache 都是使用這套軟體來進行 SSL/TLS 加密。但近期 OpenSSL 公告了一個漏洞（CVE-2014-0160），由於這個漏洞存在 OpenSSL 的 TLS/DTLS 傳輸安全層的 heartbeat（心跳）擴充功能之中，該漏洞受到攻擊時會造成記憶體內容的外洩，因此研究人員將它命名為 Heartbleed(心臟淌血)。受影響的版本為 OpenSSL 1.0.1 到 1.0.1f，目前 OpenSSL 並已釋出 OpenSSL 1.0.1g 修補該漏洞。

Openfind 資安團隊接獲通知後，便在第一時間詳細調查受影響的產品範圍，確認只有 Mail2000 6.0 SP3 版本需要修補，而相關的安全性修正程式(Security Patch)也已經迅速完成，以避免客戶遭受到不必要的惡意攻擊。

更新方法

請下載官網上的更新程式並進行下列步驟更新：

1. 請用 webmail 帳號登入 Mail2000 系統 Console

2. 將修正程式上傳

3. 解壓縮檔案

```
$ tar zxvf m2kpatchv60ms_Linux.20140410.tgz
```

4. 使用 webmail 權限執行該修正程式

```
$ cd m2kpatchv60ms_Linux
$ ./fix_heartbleed.pl
```

5. 檢查服務是否有正常起動

```
$ ps axuw | grep httpd
```

如果有出現下列執行緒則代表已完成更換並起動服務

```
webmail   20784   0.0 0.3   5256   1992 S    05:01 0:00 /webmail/httpd/bin/httpd -k start
webmail   20785   0.0 0.3   5240   1992 S    05:01 0:00 /webmail/httpd/bin/httpd -k start
…….
```

如果沒有顯示執行緒列表則請手動下指令重起服務

```
$ /webmail/httpd/bin/apachectl start
```

6. 完成

網擎資訊軟體股份有限公司

地　　址：台北市 103 重慶北路二段 243 號 7 樓
電　　話：02-2553-2000　　傳　　真：02-2553-0707
網　　址：http://www.openfind.com
E-mail： m2k_noc@openfind.com