Openfind
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.

2014.10.17

前言

近期 Google 揭露 SSL v3 有設計方面的缺陷，該弱點會導致駭客在客戶與伺服器兩端均使用 SSL v3 加密協定建立連線時，進行中間人攻擊。透過攔截與修改 HTTPS 封包，便可嘗試向伺服器主機建立連線，進而獲取使用者的相關傳輸數據與機敏資訊(cookies, and/or authorization header contents)。美國國家標準技術研究所(NIST)的國家弱點資料庫(NVD)也正式命名該弱點編號為 CVE-2014-3566。

修補方法

Mail2000 / MailGates / MailBase 的 HTTPS 須進行以下修正：

1. 修改 Apache 設定檔
   Mail2000 路徑: /webmail/httpd/conf/extra/m2k_ssl.conf
   MailGates 路徑: /mailgates/httpd/conf/extra/mg_ssl.conf
   MailBase路徑: /webmail/httpd/conf/extra/httpd-ssl.conf

2. 找到類似 SSLProtocol -all +SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2
   修改成 SSLProtocol -all +TLSv1 +TLSv1.1 +TLSv1.2

3. 然後重啟 Apache 服務。修正完成後，會影響 IE6 的使用者將無法使用 HTTPS 連線，因 IE6 不支援 TLS。

SecuShare 的 HTTPS 須進行以下修正：

1. 修改 Nginx 設定檔
   SecuShare 路徑：/webmail/scs/nginx/conf/nginx.con

2. 找到類似
   Server { …..}
   修改成
   ssl_protocols TLSv1 TLSv1.1 TLSv1.2

3. 重啟 Nginx 服務

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