

Openfind 郵件安全威脅與潛在資安風險通報

編號：OF-ISAC-15-001

Openfind 郵件安全威脅與潛在資安風險通報

Openfind 專注於郵件安全領域已經有 17 年以上的豐富經驗，致力提供客戶穩定、安全、可靠的郵件安全系統與服務。為提昇客戶郵件安全意識與避免潛在資安風險擴大，Openfind 郵件安全研究團隊將不定期提供客戶有關郵件安全威脅的即時訊息，以及潛在資安風險的警示通報。

如果您在使用 Openfind 各項產品時，有發現任何郵件安全威脅或潛在資安風險，也歡迎您透過 m2k_noc@openfind.com.tw 與我們聯繫。Openfind 技術團隊將提供您即時的資安諮詢與更新服務。

公告日期：2015 / 04 / 07

威脅名稱：XSS 修補

威脅程度：2（分數 1~5，5 代表資安事件威脅程度很高）

影響產品版本：Mail2000、MailBase、MailGates 與 MailAudit

事件摘要：

Mail2000、MailBase、MailGates 與 MailAudit 這四項產品，發現若信件內容出現特殊格式且超級大量的文字內容，則有機會造成 XSS 攻擊發生，雖然目前沒有造成任何災情的發生，但 Openfind 的資安團隊已經主動提供相關的安全性修補程式，客戶可透過更新 Patch 的方式進行處理，在官網上（<http://www.openfind.com.tw/taiwan/support/resource/update.html>）也已經提供相關的資訊給客戶參考。

修補方法：

Mail2000 程式更新

標準版：

Mail2000 V45：

請依客製版處理方式確認版本，並通知網擎資訊。

Mail2000 V60：

請由線上更新頁面，依序更新 Patch 至 SP4 第 107 (150119_1) 包。

客製版：

確認系統版本

\$ cat /webmail/etc/m2kpatch.info

V45
m2kv45_patch_0812311124 2009/02/12 18:08:28
m2kv45_patch_0810221925 2009/06/17 17:37:11
V60
mp601412221626 2015/01/06 14:41:21
mp601412261508 2015/01/06 14:41:51

提供版號給網擎資訊，由網擎資訊提供安全性程式更新包。

MailBase 程式更新

確認系統版本

\$ cat /webmail/mbase/etc/version

V4
4.0_sp2_r5248_tw

提供版號給網擎資訊，由網擎資訊提供安全性程式更新包。

MailAudit 程式更新

確認系統版本

\$ cat /mailgates/mg/etc/version

V40
mo-4.2.1-i386-linux
b07311038 1406775218 20140731-105338

提供版號給網擎資訊，由網擎資訊提供安全性程式更新包。

MailGates 程式更新

確認系統版本

\$ cat /mailgates/mg/etc/version

V4
mg-4.0.9-i386-linux
b06110921 1370915181 20130611-094621

提供版號給網擎資訊，由網擎資訊提供安全性程式更新包。

關於 Openfind 電子郵件威脅實驗室

隨著資訊安全威脅日益升高，所有資訊系統都面臨相當嚴峻的挑戰。其中，電子郵件系統更是諸多資安威脅中首當其衝的主要標的。由於資訊安全的範圍相當廣泛與多元，在實際的案例中，客戶只需要定期更新 Patch 與升級系統，結合 Openfind 主動式安全偵測服務，便可避免暴露於風險之中。Openfind 本著服務客戶的精神，不但會繼續強化產品在資安上的防護與感知能力，也會持續嚴格監控產品的安全。Openfind 電子郵件威脅實驗室也會不定期更新網路上重大的電子郵件安全威脅訊息，幫助管理者掌握最新的資安趨勢與脈動。