Open Webmail 郵件系統
安全管理與防護指南

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 11 月

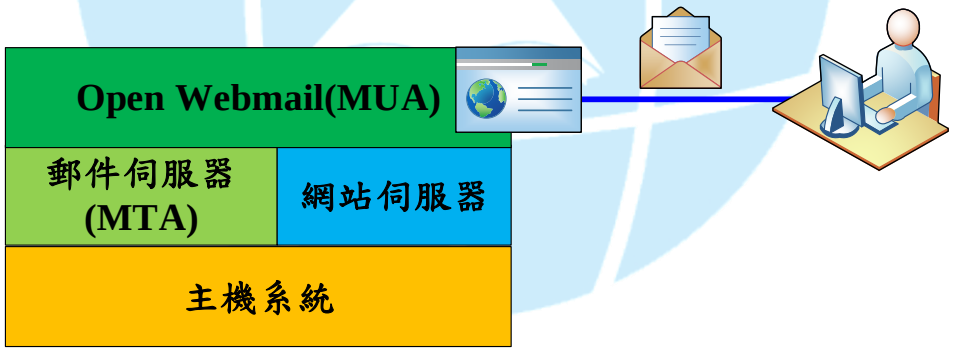
一、前言

國內有多所機關學校均建置 Open Webmail 系統來提供相關的電子郵件網路服務，為避免該系統之漏洞導致使用者電子郵件信箱遭駭，本文將說明 Open Webmail 曾被證實的重大安全漏洞，並提供相關的防禦建議，期使能降低因使用 Open Webmail 而造成的安全威脅程度。

由於 Open Webmail 相依於郵件伺服器的服務，因此在本文中也會說明郵件伺服器及主機系統的安全威脅及建議措施，提供多個面向的防護建議。

二、Open Webmail 電子郵件服務系統說明

一般常見的 Open Webmail 電子郵件網路服務相關架構如下圖所示，其中架構圖中的各個角色分別敘述說明如下。



1.主機系統

電子郵件網路服務所在主機上所使用的作業系統，例如：Linux 或 Windows 作業系統。

2. MTA (Mail Transfer Agent)

郵件傳送代理程式，又可稱為電子郵件伺服器或 SMTP（Simple Mail Transfer Protocol）伺服器（在本文中，將簡稱為郵件伺服器），其主要的功能如下所述：

(1) 寄送電子郵件

就如同現實生活中郵局的角色，幫忙寄件者將電子郵件寄送到寄件者所在的郵件伺服器。

(2) 接收其它郵件伺服器所傳遞過來的電子郵件

當郵件伺服器取得對方所傳遞過來的電子郵件後，即會交由 MDA（Mail Deliver Agent，郵遞送代理人）處理，並將所收到的電子郵件投送到相對應的帳戶下的郵件檔案中（通常為 Mailbox 格式或 mailDir 格式)以提供郵件伺服器的使用者取回電子郵件。

目前實務上所常用的郵件伺服器為 postfix 及 sendmail 郵件伺服器。

3. MUA (Mail User Agent)

郵件使用代理程式，簡單講就是我們在寄信或收信所使用的收發信軟體（例如 outlook 軟體），使用者利用 **MUA** 來建立電子郵件並寄出電子郵件或利用 **MUA** 來收取郵件伺服器上的電子郵件。本文所說明的 Open Webmail 軟體即為一種 **MUA** 軟體。與常用的 outlook 軟體不同的是，Open Webmail 是一種網頁應用程式，使用者並不需安裝任何軟體，而是使用瀏覽器即可完成寄信與收信等基本的電子郵件服務。

三、主機系統安全管理說明

在電子郵件服務系統架構中，主機系統為最底層之架構。因此，維護主機系統之安全為首要之任務。一旦主機系統遭受到資安的威脅，架構於其上的電子郵件服務系統同樣也將面臨相關的資安風險，為有效降低主機系統所面臨的資安風險，相關建議如下：

1. 系統主機應安裝防火牆，以及阻絕不使用之網路通訊埠（例如：網站伺服器應僅開放通訊埠 80 或 443），並定期檢視防火牆相關規則是否符合資安要求。
2. 系統主機應安裝防毒軟體，除了需更新至最新版的病毒碼外，建議也能提供系統即時的檢查防護。
3. 系統主機需能進行作業系統與相關軟體之更新和修補，並定期或不定期進行主機弱點掃描，以期即時找出系統潛在的漏洞。
4. 當管理人員在遠端進行伺服器主機系統維護時，應在加密管道進行（例如：使用 SSH 而非使用 TELNET 不安全的連線），並應限制可維護系統的來源範圍(例如：限定某個 IP 可進行連線)。
5. 建議系統維護人員不要使用遠端遙控軟體(例如:遠端桌面)進行系統管理、維護或更新。
6. 當系統管理者利用主控台（Console）進行維護，在離開現場前需登出主控台。
7. 登入主控台（Console）的密碼建議不要使用原廠所設定的預設密碼。
8. 系統主機因實務需要而需建立分享功能（例如：網路芳鄰），應先建立網路及主機之安全控制措施。
9. 系統主機應定期依照人事異動情形進行實際使用權限之調整，以及變更使用者權限。
10. 系統主機應定期盤點帳號，並移除不相關的帳號。
11. 系統主機應準備適當及足夠之備援設施，定期執行必要之資料與軟體備份及備援作業，以確保在意外發生時，可迅速回復正常作業。
12. 依實際需求保存伺服器主機在運作時所產生的相關記錄檔案。

四、Open Webmail 安全漏洞

為了讓使用者能夠更便利的使用郵件伺服器的功能，管理者通常會建立 Web Mail 服務，讓使用者能夠便利地利用瀏覽器，即可使用郵件服務來寄信或收信，而 Open Webmail (官方網站：https://openwebmail.org/)即是開源碼社群中一套頗富盛名的 WEB MAIL 軟體。因此，有不少的學校機關會選擇此套軟體來建置 Web Mail 服務，但也因使用者眾多，常成為惡意攻擊者攻擊的目標，有鑑於此，在本文中將說明 Open Webmail 曾被證實的相關漏洞與建議預防方式。在此將以 CVE（Common Vulnerabilities and Exposures）組織所承認，並收錄之嚴重漏洞為主要說明對象。以 Open Webmail 軟體而言，曾被揭露並證實的重大漏洞如下所述。

1. CVE-2004-2284

項目	內容
影響範圍	攻擊者可遠端利用此弱點，在系統上執行任意指令。
影響版本	2.32 之前的版本。
弱點成因	在 vacation.pl 程式中的 read_list_from_file 函數，由於未對輸入的參數實施有效適當的過濾，導致惡意的使用者可利用在參數上輸入惡意的指令（例如 shell 指令），即可成功的在 Open Webmail 所在的主機上執行此惡意指令。
建議事項	建議更新至 2.32 之後的版本，如果在實務上無法更新版本，也可至下列網址取得更正檔來對 vacation.pl 進行更新。 http://openwebmail.org/openwebmail/download/cert/patches/SA-04:04/vaca tion.pl.patch

2. CVE-2005-1435

項目	內容
影響範圍	攻擊者可遠端利用此弱點，在系統上執行任意指令。
影響版本	2.51 之前的版本。
弱點成因	在使用者登入的情況下，由於程式所使用的開檔函數(名稱為 open)，並未適當的對輸入的參數實施有效的過濾，導致如果所欲開啟的檔案，其檔案名稱具有如 shell 指令的名稱，在利用 open 開啟檔案的過程中，當解析到檔案名稱時，即會在 Open Webmail 所在的主機上執行檔案名稱中所夾帶的 shell 指令。
建議事項	建議更新至 2.51 之後的版本。

3. CVE-2005-1435

項目	內容
影響範圍	攻擊者可遠端利用此弱點，在系統上執行任意腳本指令。
影響版本	2.51 之前的版本。
弱點成因	Open Webmail 2.51 之前版本存在跨網站腳本攻擊(Cross Site Script，XSS)漏洞，遠端攻擊者可以借助 openwebmail-send.pl，openwebmail-advsearch.pl，openwebmail-folder.pl，openwebmail-prefs.pl，openwebmail-abook.pl，openwebmail-read.pl，openwebmail-cal.pl 等具有此漏洞的程式，注入任意惡意腳本程式(Script)，即可經由此類腳本程式觸發 XSS 攻擊。
建議事項	建議更新至 2.51 之後的版本。

除了上述較為嚴重的漏洞外，另外還有其它較為次要輕微的漏洞，使用者可查看下列網址，以取得更詳盡的資訊。

https://www.cvedetails.com/vulnerability-list/vendor_id-1329/Open-Webm

ail.html

五、郵件服務系統安全

郵件服務系統主要是由 MUA 及郵件伺服器所組成，而其中 MUA(例如本文中的 Open Webmail)因直接被使用者所接觸，所以常成為被攻擊的目標，除此之外，郵件伺服器也常是攻擊的目標。因此，郵件伺服器的安全維護也是不可輕忽的議題。由於郵件系統的特殊性，在一般的情況下，郵件系統會服務大量成員，這也就意味著在郵件伺服器上會存在大量的帳號，在此種情況下，維護郵件伺服器上的帳號安全即成為相當重要的課題。因為一旦帳號被入侵，攻擊者不僅能夠取得該使用者的電子郵件資訊，甚至也會取得郵件伺服器所在主機上一般使用者的權限，所以維護郵件伺服器的帳號安全應為首要之任務。

在關於維護帳號安全的規範上，使用者可參考 NIST(National Institute of Standards and Technology, 國家標準暨技術研究院)所發佈的編號 sp800-63 之數位認證建議安全規範。此規範的相關網址如下 https://pages.nist.gov/800-63-3/，它讓使用者有相關標準規範可遵循。在規範中所提出最重要的重點即是使用者密碼的複雜度，設定太簡單即成為弱密碼，很容易被猜測到而造成密碼外洩的資安危機。在實務上有很多的入侵資安事件，都是因為使用者設定不適當的弱密碼所致，如同下表 splashdata 密碼安全公司(官方網址為 https://www.splashdata.com/)在 2018 年所統計的弱密碼排行所呈現。

名次	弱密碼
1	123456
2	password
3	123456789
4	12345678
5	12345

名次	弱密碼
6	111111
7	1234567
8	sunshine
9	qwerty
10	iloveyou

對於密碼複雜度的要求，在過去總是會建議需具備英數字，甚至於特殊字元的建議(常導致使用者無法有效的記憶)，但近來有越來越多的研究顯示，設定長度較長的密碼更能增進安全的效益。因此，會建議要特別著重在密碼的長度。另外，在定期更換密碼的政策方面，則要求使用者每隔一段時間即更換密碼，此類政策是否真能達到增進資訊安全的效益，也是目前所被討論，甚至被質疑。微軟在近期內欲在作業系統中移除「要求定期變更密碼的密碼過期政策」的功能(相關新聞：https://www.ithome.com.tw/news/130226) ，或許正是回應此類政策的質疑。但目前「定期更改密碼」政策是否必要，尚未形成共識，所以此類政策的實施還是必須回歸至組織的資安政策而定。

由於開源碼軟體的盛行，有越來越多的組織會採用開源碼的解決方案來完成網路服務的建置。開源碼軟體雖具有開放多元的特性，但其最大的問題在於其更新軟體的機制並不夠友善，所以並不能像微軟系統一樣，只要一鍵即可完成更新，也因此大部份的使用者在建置完成後，即不再更新。因而造成許多潛在的資安問題，所以必須提醒管理者在使用開源碼軟體完成網路服務建置後，必須經常至該開源碼軟體的官方網站上查看是否有新的安全通報。如果有重大的安全通報，即需評估更新版本的必要性。以郵件系統為例，最常使用的郵件伺服器即為 Postfix，其官方網址為 http://www.postfix.org/，Postfix 的誕生，其實是為了修正 Sendmail (一個最老牌的郵件伺服器)難以上手的問題而開發出來的軟體，由於其效能優異及易於上手（相對於 Sendmail 而言）的特性，而漸漸地廣為人所用，也因此

常為惡意攻擊者所狙擊的目標。因此，建議相關管理者應經常至 Postfix 官方網站上查看是否有重大的漏洞，以及是否有相關更新檔的資訊，來即時修正 Postfix 的漏洞。簡而言之，關於維護郵件伺服器安全的相關建議如下：

1. 由於開源碼軟體的更新機制並不完善，因此在使用開源碼軟體的情況下，建議管理者應定時至該開源碼軟體的官方網站確認是否有相關的安全修正程式，並評估實作更新的必要性，若為商業軟體也應定時使用其更新機制來進行更新。
2. 定時針對該軟體實施弱點掃描，並依其掃描結果進行修正。
3. 定時盤點郵件伺服器的帳號清冊，並移除不必要的帳號。
4. 宣導並確認使用者帳號並未使用弱密碼。

六、結論

隨著開源碼軟體的盛行，有越來越多的機關學校會採用相關開源碼的解決方案來提供具有 WEB MAIL 功能的電子郵件服務。對於此類的解決方案所提供的安全建議如下：

1. 如果提供 Web Mail 功能，建議需採用支持 SSL 的網站服務（即使用者使用 https 連線）來對傳輸過程的資訊進行加密，以避免在登入過程中所輸入帳號及密碼被惡意使用者所擷取，而造成帳號密碼資訊外洩。
2. 需隨時留意所採用的開源碼軟體是否有重大的安全漏洞被發佈，並視實務情況來進行版本更新。
3. 建議時常留意 CVE(https://cve.mitre.org/)組織資訊，確認所採用的開源碼軟體是否有相關 CVE 資訊。
4. 需定時清查郵件伺服器上的帳號，確認無幽靈帳號。
5. 建議要求長字串的帳號密碼（最少 8 碼以上）。
6. 限定郵件伺服器可登入的來源範圍，在實務上，我們通常會利用 SSH

來登入郵件伺服器進行系統管理，如果非必要，建議限定可登入的來源範圍。

7. 定時實施系統弱點掃描，並評估進行系統修補。
8. 針對提供 Web Mail 功能的軟體(例如: Open Webmail)進行網頁程式漏洞掃描，並根據其報告進行安全修正。

七、參考資料

1. Open Webmail 官方網站
https://openwebmail.org/
2. Open Webmail: Security Vulnerabilities
https://www.cvedetails.com/vulnerability-list/vendor_id-1329/Open-Webmail.html
3. 國家標準暨技術研究院(NIST)之數位認證建議安全規範
https://pages.nist.gov/800-63-3/
4. 不必再定期改密碼了！Windows 桌機及 Server 版可望拿掉密碼過期政策
https://www.ithome.com.tw/news/130226
5. Postfix 官方網站
http://www.postfix.org/