行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2019-0048	發布時間	Thu Apr 25 14:41:51 CST 2019
事件類型	漏洞預警	發現時間	Thu Apr 25 00:00:00 CST 2019
警訊名稱	PHP 的 imap_open 函式存在安全漏洞(CVE-2018-19518)，允許攻擊者遠端執行任意程式碼，請儘速確認並調整設定		
內容說明	PHP 的 imap_open 函式存在安全性漏洞，導致攻擊者可繞過身份驗證於目標系統上執行任意程式碼。 imap_open 函式為開啟使用者的 MAILBOX(信箱)之 IMAP 串流，其預設 MAILBOX 參數傳遞給 rsh 或 ssh 前未經過任何過濾或確認，因此攻擊者可繞過禁用函式限制，在目標系統上執行任意執行碼。		
影響平台	PHP 5.6.0 至 PHP 5.6.38 PHP 7.0.0 至 PHP 7.0.32 PHP 7.1.0 至 PHP 7.1.24 PHP 7.2.0 至 PHP 7.2.12		
影響等級	中		
建議措施	1.確認目前所使用之系統中是否存在該函式，與該函式存在之必要性。 2.修改/移除使用該函式之套裝系統上的預設帳號密碼，選用符合複雜性需求之密碼並定期更換。 3.從防火牆設置阻擋來自外部存取該資訊設備/網站的所有連線，如有特殊情況必須從外部連線存取時，透過防火牆設定白名單的方式開放連線。 4.若評估後仍需使用該函式，可參考以下建議事項： a.檢查並過濾傳入 imap_open 函式中的特殊字元。 b.在呼叫 imap_open 函式時，強制使用/norsh 選項。		

	c.在 PHP 設定檔(php.ini)中將 imap.enable_insecure_rsh 值設置為 0。 5.若評估後無需使用該函式，可參考以下建議事項： a.於 PHP 設定中停用 IMAP 模組。 b.在 PHP 設定檔(php.ini)中將 imap_open 加入 disable_functions 區塊中。
參考資料	1. https://nvd.nist.gov/vuln/detail/CVE-2018-19518 2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19518 3. https://github.com/Bo0oM/PHP_imap_open_exploit

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw