張貼日期：2022/10/07

【資安漏洞預警】微軟Microsoft Exchange Server存在安全漏洞(CVE-2022-41040與CVE-2022-41082)，允許攻擊者遠端執行任意程式碼，請儘速確認並評估採取緩解措施

- 主旨說明：微軟Microsoft Exchange Server存在安全漏洞(CVE-2022-41040與CVE-2022-41082)，允許攻擊者遠端執行任意程式碼，請儘速確認並評估採取緩解措施

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202210-0333，
  - 研究人員發現Microsoft Exchange Server存在ProxyNotShell安全漏洞，分別為伺服器端請求偽造(SSRF)漏洞(CVE-2022-41040)與PowerShell遠端執行程式碼(RCE)漏洞(CVE-2022-41082)，遠端攻擊者可串連上述漏洞繞過身分驗證機制並提升權限後，進而遠端執行任意程式碼。
- 影響平台：
  - Microsoft Exchange Server 2013 Cumulative Update 23
  - Microsoft Exchange Server 2016 Cumulative Update 22，23
  - Microsoft Exchange Server 2019 Cumulative Update 11，12
- 建議措施：
  1. 目前微軟官方尚未針對此漏洞釋出更新程式，建議評估是否先行採取緩解措施，執行步驟如下：
     1. 開啟IIS管理員。
     2. 選擇「Default Web Site」。
     3. 於右側功能列中點擊「URL Rewrite」。
     4. 於右側操作窗格動作中點擊「新增規則」。
     5. 選擇「要求封鎖」並按下「確定」。
     6. 於「模式(URL路徑)」欄位新增字串「.*autodiscover.json.*Powershell.*」。
     7. 於「使用」下拉式選單選擇「規則運算式」。
     8. 於「封鎖方式」下拉式選單選擇「中止要求」並按下「確定」。
     9. 展開並點擊規則進行編輯，在「檢查輸入字串是否為」下拉式選單選擇「符合模式」，確認「模式」欄位內容為「.*autodiscover.json.*Powershell.*」。
     10. 將「條件輸入」欄位內容由「{URL}」修改為「{REQUEST_URI}」並按下「確定」。 註：若需變更任何規則，建議刪除既有規則並重新建立。
  2. 請持續注意微軟官方資訊，並於釋出修補程式後儘速安裝
     1. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41040
     2. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41082
- 參考資料：
  1. https://thehackernews.com/2022/10/mitigation-for-exchange-zero-days.html?m=1
  2. https://www.ithome.com.tw/news/153387
  3. https://www.ithome.com.tw/news/153457
  4. https://nvd.nist.gov/vuln/detail/CVE-2022-41040
  5. https://nvd.nist.gov/vuln/detail/CVE-2022-41082
  6. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41040

7. https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41082
8. https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/
9. https://www.microsoft.com/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/

計算機與通訊中心
網路系統組 敬啟