張貼日期：2022/10/03

【資安漏洞預警】駭客攻陷微軟Exchange伺服器的RCE零時差漏洞

- 主旨說明：駭客攻陷微軟Exchange伺服器的RCE零時差漏洞

- 內容說明：
  - 轉發 科學園區資安資訊分享與分析中心 SPISAC-ANA-202210-0002。
  - 越南資安業者GTSC指出，該公司在微軟的Exchange伺服器上發現了一個已遭開採的零時差遠端程式攻擊漏洞，迄今已確定至少已有一家以上的組織受害，並擔心有其它受害組織並不知道自己已被駭客入侵。
  - GTSC提供的是安全監控中心（Security Operations Center，SOC，即服務（SOC as a Service））其SOC團隊在今年8月初發現Exchange伺服器遭到攻擊，調查之後才發現駭客所利用的是一個尚未被公開的零時差漏洞。收到通報的趨勢科技Zero Day Initiative（ZDI）團隊已驗證過該漏洞，並認為它涉及兩個安全漏洞，ZDI賦予這兩個漏洞的暫時性編號為ZDI-CAN-18333與ZDI-CAN-18802，CVSS風險等級分別是8.8與6.3。
  - 根據GTSC的分析，駭客的攻擊手法類似針對ProxyShell漏洞的攻擊，且該公司團隊已成功複製如何利用該漏洞存取Exchange後端元件，進而執行遠端程式攻擊。此外，駭客不僅於受害系統上建立了據點，也透過不同的技術打造了後門，並於受害系統上橫向移動至其它伺服器，GTSC也偵測到駭客使用了於中國熱門的Web Shell跨平臺開源管理工具Antsword，來管理於受害Exchange伺服器上所植入的Web Shell。
- 影響平台：
  Microsoft Exchange Server 2013/2016/2019
- 建議措施：
  - GTSC提出了暫時性補救措施，建議組織可於IIS伺服器上的URL Rewrite Rule模組上新增規則，以封鎖帶有攻擊指標的請求。
  - 微軟也對此漏洞公布了緩解措施與檢測指南，建議Microsoft Exchange Server 2013/2016/2019的用戶，在微軟釋出更新修補前，可以採取這些行動。
- 參考資料：
  1. https://www.ithome.com.tw/news/153387
  2. https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

計算機與通訊中心
網路系統組 敬啟