張貼日期：2020/12/11

【資安訊息】網路安全廠商FireEye紅隊安全測試工具遭外流，建議儘速修補該套工具所利用之CVE安全漏洞！

主旨：【資安訊息】網路安全廠商FireEye紅隊安全測試工具遭外流，建議儘速修補該套工具所利用之CVE安全漏洞！

- 內容說明：
  - 轉發 行政院國家資通安全會報技術服務中心 資安訊息警訊 NISAC-ANA-202012-0496
  - 網路安全廠商FireEye於12月8日公布近日該公司紅隊所使用之安全測試工具遭外流，這套工具無零時差漏洞攻擊程式，皆為已存在修補方式之CVE安全漏洞。
  - FireEye已在GitHub上公開利用該套工具偵測規則(包含Snort、Yara、ClamAV及HXIOC)供大眾參考使用或部署。
- 影響平台：
  以下為測試工具所利用之16個CVE安全漏洞與對應之設備或產品：
  1. CVE-2014-1812 – Windows Local Privilege Escalation
  2. CVE-2016-0167 – local privilege escalation on older versions of Microsoft Windows
  3. CVE-2017-11774 – RCE in Microsoft Outlook via crafted document execution (phishing)
  4. CVE-2018-8581 - Microsoft Exchange Server escalation of privileges
  5. CVE-2019-0604 – RCE for Microsoft Sharepoint
  6. CVE-2019-0708 – RCE of Windows Remote Desktop Services (RDS)
  7. CVE-2020-0688 – Remote Command Execution in Microsoft Exchange
  8. CVE-2020-1472 – Microsoft Active Directory escalation of privileges
  9. CVE-2019-8394 – arbitrary pre-auth file upload to ZoHo ManageEngine ServiceDesk Plus
  10. CVE-2020-10189 – RCE for ZoHo ManageEngine Desktop Central
  11. CVE-2018-13379 – pre-auth arbitrary file reading from Fortinet Fortigate SSL VPN
  12. CVE-2018-15961 – RCE via Adobe ColdFusion (arbitrary file upload that can be used to upload a JSP web shell)
  13. CVE-2019-3398 – Confluence Authenticated Remote Code Execution
  14. CVE-2019-11510 – pre-auth arbitrary file reading from Pulse Secure SSL VPNs
  15. CVE-2019-11580 - Atlassian Crowd Remote Code Execution
  16. CVE-2019-19781 – RCE of Citrix Application Delivery Controller and Citrix Gateway
- 建議措施：
  1. 建議機關檢視內部是否使用上述設備或產品，並確認其修補或更新狀態，若未進行修補或更新應盡速完成，避免未來可能被作為該套工具攻擊之對象。
  2. 若未能即時完成修補或更新，建議將FireEye已在GitHub上公開利用該些工具之Snort、Yara、ClamAV或及HXIOC部署於資安防護設備中，用以偵測或封鎖該套工具的攻擊。
- 參考資料：
  1. http://cs-notices.fireeye.com/webmail/484561/315422185/88b9986cd9e2bb55e59d28a46b00470df398125330916b5dffa37f6b987de151
  2. https://github.com/fireeye/red_team_tool_countermeasures/blob/master/CVEs_red_team_tools.md
  3. https://github.com/fireeye/red_team_tool_countermeasures

計算機與通訊中心
網路系統組 敬啟