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-2020-0134	發布時間	Thu Dec 10 16:56:37 CST 2020
事件類型	攻擊活動預警	發現時間	Wed Dec 09 00:00:00 CST 2020
警訊名稱	網路安全廠商 FireEye 紅隊安全測試工具遭外流，建議機關儘速修補該套工具所利用之 CVE 安全漏洞		
內容說明	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。 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 th at 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 SS L VPNs 15. CVE-2019-11580 - Atlassian Crowd Remote Code Execution 16. CVE-2019-19781 – RCE of Citrix Application Delivery Controller and Citrix Gateway
影響平台	無
影響等級	中
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

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