區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 資安案例分享
  - 資安情資分析
  - WINDOWS SMBv3 嚴重漏洞
  - Tomcat Server Ghostcat漏洞
  - DrayTek 路由器漏洞
  - DDoS 大流量攻擊

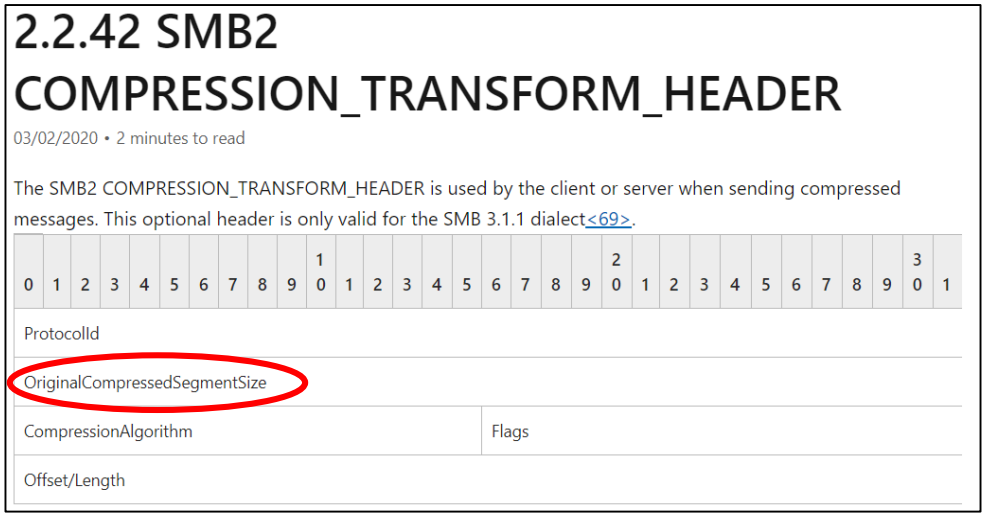
WINDOWS SMBv3 嚴重漏洞

CVE-2020-0796 漏洞簡介

- 3/10微軟周二修補程式日(Patch Tuesday)的更新修補中，漏修補Server Message Block 3.1.1 (SMBv3)漏洞
- 此漏洞的嚴重程度與永恆之藍(EternalBlue)攻擊程式所利用的CVE-2017-0145一樣危險
- 在Github上已經有數個PoC程式去驗證此漏洞
- 如果此漏洞遭人利用而發動攻擊，極可能會發生跟WannaCry同樣等級的災難

漏洞原因

- 漏洞發生在srv2.sys檔案的 Srv2DecompressData函式
- 由於SMBv3在傳送資料前會壓縮資料，並在記憶體中配置一個解壓縮緩衝區(Buffer)
- 而傳送資料的過程中上述的函式並沒有檢查封包長度，導致攻擊者可設計異常的封包長度(紅圈處)，造成緩衝區發生溢位(overflow)



2.2.42 SMB2 COMPRESSION_TRANSFORM_HEADER

03/02/2020 • 2 minutes to read

The SMB2 COMPRESSION_TRANSFORM_HEADER is used by the client or server when sending compressed messages. This optional header is only valid for the SMB 3.1.1 dialect<69>.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
ProtocolId																															
OriginalCompressedSegmentSize																															
CompressionAlgorithm																Flags															
Offset/Length																															

資料來源：https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/1d435f21-9a21-4f4c-828e-624a176cf2a0

影響版本

- 此漏洞會影響使用SMBv3服務的作業系統：
  - Windows 10 Version 1903/1909
  - Windows Server Version 1903/1909

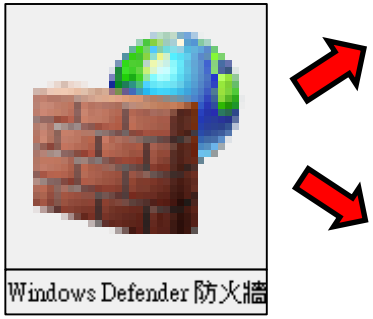
備註： Windows 7 與 Windows Server 2008 R2 以前的版本，SMBv2, SMBv1不會受到此漏洞影響。但如果沒有使用上的需求，建議關閉SMB相關服務來降低被攻擊的風險。

緩解措施

- 由微軟提供的緩解辦法，如果因某些原因無法更新時，請先執行以下的方式限制漏洞的發生：

1. 開啟Windows內建防火牆，並且限制或阻擋tcp port 445有關的連線
2. 禁用SMBv3壓縮功能，用管理員權限開啟PowerShell，輸入下面指令(完成後不用重開機)

➢ Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force



輸入規則

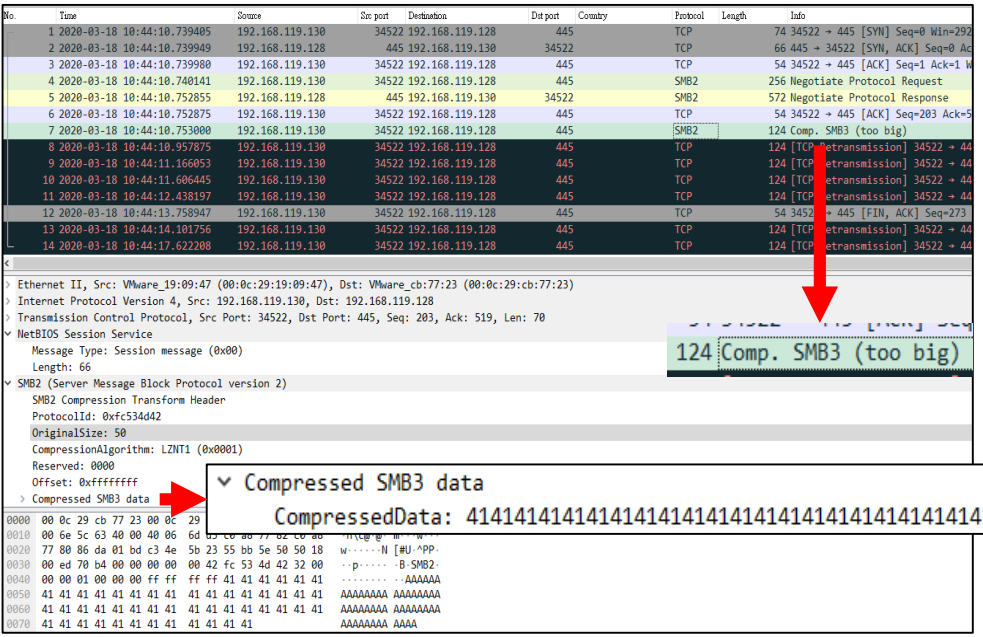
Netlogon 服務 (NP-In)	Netlogon 服務	全部	否	允許	否	Syst...	任一	任一	TCP	445
遠端事件記錄檔管理 (NP-In)	遠端事件記錄檔管理	私人, ...	否	允許	否	Syst...	任一	本機子網路	TCP	445
遠端事件記錄檔管理 (NP-In)	遠端事件記錄檔管理	網域	否	允許	否	Syst...	任一	任一	TCP	445
遠端服務管理 (NP-In)	遠端服務管理	網域	否	允許	否	Syst...	任一	任一	TCP	445
遠端服務管理 (NP-In)	遠端服務管理	私人, ...	否	允許	否	Syst...	任一	本機子網路	TCP	445
檔案及印表機共用 (SMB-In)	檔案及印表機共用	私人, ...	否	允許	否	Syst...	任一	本機子網路	TCP	445
檔案及印表機共用 (SMB-In)	檔案及印表機共用	網域	否	允許	否	Syst...	任一	任一	TCP	445

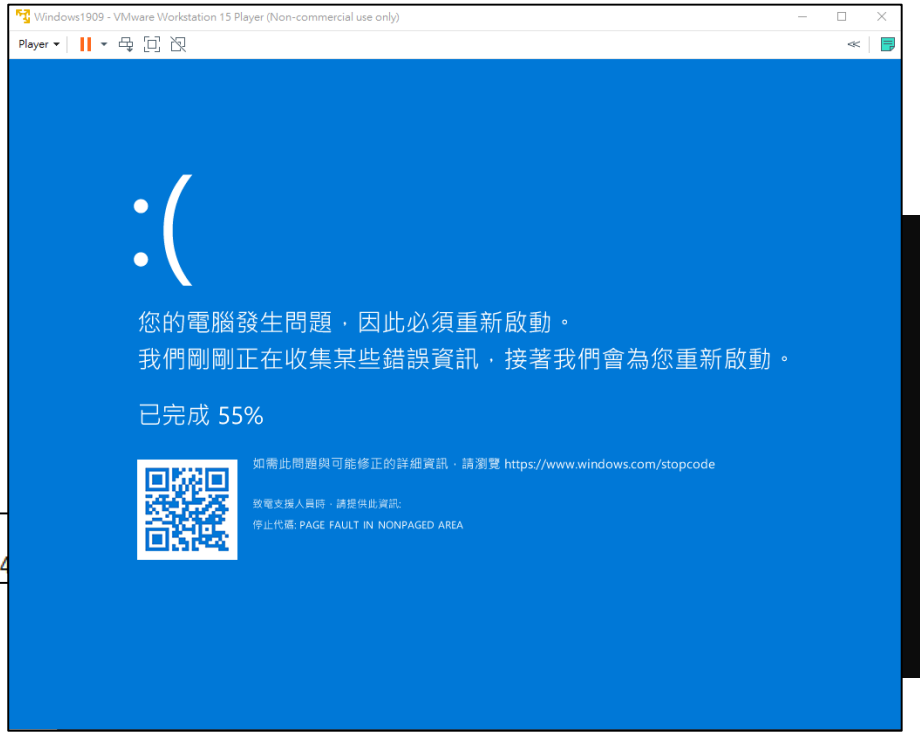
輸出規則

核心網路功能 - 群組原則 (NP-Out)	核心網路功能	網域	是	封鎖	否	Syst...	任一	任一	TCP	任一	445
檔案及印表機共用 (SMB-Out)	檔案及印表機共用	網域	否	允許	否	Syst...	任一	任一	TCP	任一	445
檔案及印表機共用 (SMB-Out)	檔案及印表機共用	私人, ...	否	允許	否	Syst...	任一	本機子網路	TCP	任一	445

PoC程式測試

- 從PoC程式得知，SMB的封包長度是可以被攻擊者設計
- 如電腦未修補此漏洞，攻擊者發送異常封包攻擊漏洞
- 某一個PoC程式可以造成電腦異常





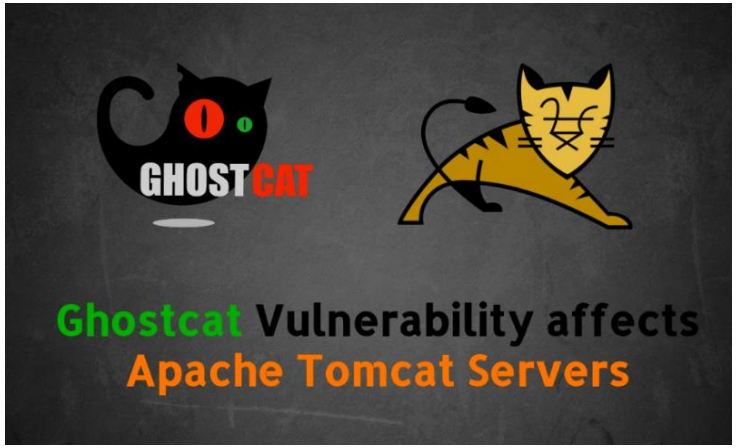
建議措施

1. 更新微軟的修補漏洞程式(下載網址：https://www.catalog.update.microsoft.com/Search.aspx?q=KB4551762)
2. 在防火牆、路由器等網路設備上設定阻擋或關閉 port 445 的連線
3. 若轄下學校未設置防火牆設備則建議，利用各區網ASR阻擋445port 連線

Tomcat Server Ghostcat漏洞

前言

- 漏洞編號：CVE-2020-1938
- 近日國內某校的圖書館網頁遭到中國駭客組織HUAPI植入後門程式，經國內業者分析發現，駭客組織是透過這個漏洞上傳惡意程式到圖書館網頁，使該網頁變成惡意程式的下載站(Download Site)
- 受到影響的Tomcat橫跨數個版本(目前確認Tomcat 6/7/8/9都會受到漏洞影響)，也稱之為Ghostcat漏洞



圖片來源：https://www.secpod.com/blog/ghostcat-vulnerability-cve-2020-1938/

漏洞描述

- Apache Tomcat AJP協議(connector)中，存在檔案的讀取/包含漏洞(read/inclusion vulnerability)
- 攻擊者可以利用此漏洞讀取Tomcat所有webapp目錄下的任意檔案，或是上傳惡意腳本程式，利用漏洞達到遠端程式碼執行(RCE)

影響範圍

- Apache Tomcat 9.x < 9.0.31
- Apache Tomcat 8.x < 8.5.51
- Apache Tomcat 7.x < 7.0.100
- Apache Tomcat 6.x

建議防護措施

- Apache Tomcat官方已經針對Tomcat 7/8/9 版本釋出對應的更新檔案修補此漏洞，請盡速至官方網站下載對應的最新版本
- 另外，官方目前並未釋出Tomcat 6.x與Tomcat 6之前的修補程式。為了降低被攻擊的風險，請盡速更換Tomcat的版本

Q & A