02_資安事件及異常紀錄 - 一般 #766

一般 # 790 (Closed-關閉): 內部自行掃描追蹤

10.15.72.146(上水 竹東)

2024-06-05 10:39 - Joy Liao

狀態:	Closed-關閉	**開始日期:**	2024-06-05
優先權:	Normal	**完成日期:**	
被分派者:	宗沛 陳	**完成百分比:**	0%
分類:		**預估工時:**	0:00 小時

概述

Microsoft Windows SMB/NETBIOS NULL 會話驗證繞過漏洞
7.5 (高)
99
%
10.15.72.146
445/TCP
2024年5月29日星期三12:48 CST
摘要
Microsoft Windows 很容易存在透過 SMB/NETBIOS 的驗證繞過漏洞。
檢測結果
可以使用空的登入名稱和密碼登入共用 " IPC$ " 。
探索
此缺陷是由於 SMB
共享造成的，允許來賓用戶進行完全存取。如果啟用來賓帳戶，任何人都可以在沒有有效使用者帳戶或密碼的情況下存取電腦。
檢測方法
細節：
Microsoft Windows SMB/NETBIOS NULL 會話驗證繞過漏洞...
物件ID：1.3.6.1.4.1.25623.1.0.801991
使用版本：
2023-07-28T13:05:23+08:00
受影響的軟體/作業系統
- Microsoft Windows 95 - Microsoft Windows 98 - Microsoft Windows NT - Microsoft Windows 2000 - 其他實作/版本中的 Microsoft Windows
也可能受到影響
影響
成功利用該漏洞可能會讓攻擊者利用共享來導致系統崩潰。
解決方案
解決方案類型：
不會修復
自該漏洞披露以來至少一年內沒有提供任何已知的解決方案。可能不會再提供任何服務。一般解決方案選項包括升級至較新版本、停用相應功能、刪除產品或用另一產品取代該產品。
解決方法是， - 停用空會話登入。 - 刪除共享。 - 在共享上啟用密碼。
參考
CVE
CVE-1999-0519
其他
http://xforce.iss.net/xforce/xfdb/2
http://seclab.cs.ucdavis.edu/projects/testing/vulner/38.html

歷史

#1 - 2024-06-05 10:40 - Joy Liao

- 被分派者 設定為 宗沛 陳

#2 - 2024-06-25 09:54 - Joy Liao

- 父議題 設定為 #790

#3 - 2024-11-21 09:53 - Joy Liao

- 狀態 從 New-新增 變更為 Resolved-解決

#4 - 2024-11-21 09:55 - Joy Liao

- 狀態 從 Resolved-解決 變更為 Closed-關閉