**衛生福利部109年資通安全稽核作業**

**資安弱點檢測報告**

**Vulnerability Assessment Report**



**中華民國 109 年 9 月 26 日**

#### 低安全性帳號

|  |  |  |
| --- | --- | --- |
| 風險IP | 風險帳號 | 風險密碼 |
| 192.168.121.14 | dministrator | 12345 |

#### SMB系統漏洞檢測

|  |  |
| --- | --- |
| 弱點名稱 | cve\_2020\_1206 |
| 弱點敘述 | 該漏洞產生的原因是SMB的解壓縮函數Srv2DecompressData在處理發送給目標SMBv3服務器以偽造的息請求時，所產生問題，攻擊者可以讀取未初始化的kernel內存，還可以對壓縮函數進行修改。 |
| 建議措施 | 用管理員身份執行命令提示字元，必輸入以下命令，Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force,此外無需重啟電腦 |
| 風險IP | * 192.168.121.147 * 192.168.121.12 * 192.168.121.173 * 192.168.121.43 * 192.168.121.200 |

|  |  |
| --- | --- |
| 弱點名稱 | cve\_2020\_0796 |
| 弱點敘述 | 該漏洞遠讓遠端攻擊者可對目標系統之SMBv3服務發送特製請求或架設惡意的SMBv3伺服器誘騙受害者進行連線，導致遠端執行任意程式碼 |
| 建議措施 | 目前微軟官方已針對此弱點釋出更新程式，請至下列連結進行更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796 |
| 風險IP | * 192.168.121.147 * 192.168.121.12 * 192.168.121.173 * 192.168.121.14 * 192.168.121.43 * 192.168.121.200 |

|  |  |
| --- | --- |
| 弱點名稱 | ms17\_010 |
| 弱點敘述 | Microsoft Server Message Block 1.0 (SMBv1) 處理特定要求的方式中存在資訊洩漏弱點。攻擊者可能會蓄意製作封包，藉此導致伺服器資訊洩漏，以及執行任意程式。例如：WanaCrypt的勒索病毒，主要透過此弱點將受感染的電腦,大量檔案加密，並且要求高價比特幣贖金來贖回資料。 |
| 建議措施 | 關閉SMB1服務，詳細操作資訊，請到以下網址，https://walker-a.com/archives/4261，Step2開始將指引您如何關閉SMB1 |
| 風險IP | * 192.168.121.147 * 192.168.121.12 * 192.168.121.173 * 192.168.121.14 * 192.168.121.43 * 192.168.121.200 |

#### 資料共享風險

|  |  |
| --- | --- |
| IP位置 | 192.168.121.14 |
| 資料夾資訊 | 資料夾路徑 |
| \\192.168.121.14\ADMIN$ |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| none |
| \\192.168.121.14\C$ |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| none |
| \\192.168.121.14\E$ |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| none |
| \\192.168.121.14\FX P255 dw |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| READ |
| \\192.168.121.14\HP-CP3525$ |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| READ |
| \\192.168.121.14\IPC$ |
| 資料夾權限 |
| Anonymous access |
| READ |
| Current user access |
| READ/WRITE |
| \\192.168.121.14\SHARPMX- |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| READ |
| \\192.168.121.14\print$ |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| READ |
| \\192.168.121.14\prnproc$ |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| READ |
| \\192.168.121.14\scan |
| 資料夾權限 |
| Anonymous access |
| none |
| Current user access |
| READ/WRITE |