**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 10 月 26 日**

* RDP檢測項目：
  + 開起服務數量
* SMB檢測項目：
  + SMB系統漏洞檢：
    1. CVE 2020-1206
    2. CVE 2020-0796
    3. MS 07-029
    4. MS 08-067
    5. MS 10-054
    6. MS 10-061
    7. MS 17-010
  + 高風險帳號
    - 風險帳號清單：

1. administrator
2. Administrator
3. user1
4. admin
5. alex
6. pos
7. demo
8. db2admin
9. Admin
10. sql
11. Root
12. Admin
13. Test
14. Guest
15. Info
16. Adm
17. Mysql
18. User
19. Administrator
20. Oracle
    * + 風險密碼清單：
21. 12345
22. 123456
23. 123456789
24. test1
25. password
26. 12345678
27. zinch
28. g\_czechout
29. asdf
30. qwerty
31. dubsmash
32. test
33. 1234567890
34. 1234567
35. Aa123456
36. iloveyou
37. 1234
38. abc123
39. 11111111
40. 123123
41. 1qaz@WSX
42. 2wsx#ED
43. 3edc$RFV
44. 4rfv%TGB
45. x
46. Zz
47. St@rt123
48. 1
49. bl4ck4ndwhite
50. admin
51. alex
52. administrator
53. .......
54. Username
55. Username123
56. 123456
57. Password
58. 1234
59. 12345
60. Passwd
61. 123
62. Test
    * 風險資料夾資訊

#### SMB低安全性帳號概況

#### SMB系統漏洞檢測概況

#### SMB資料共享風險概況

* RDP服務開啟概況

詳細資訊  
SMB低安全性帳號詳細資訊

|  |  |  |
| --- | --- | --- |
| 風險IP | 風險帳號 | 風險密碼 |

#### SMB系統漏洞檢測詳細資訊

|  |  |
| --- | --- |
| 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 | * 192.168.28.79 * 192.168.28.107 * 192.168.28.36 * 192.168.28.105 * 192.168.28.100 * 192.168.28.59 * 192.168.28.104 * 192.168.28.110 * 192.168.28.97 * 192.168.28.179 * 192.168.28.77 * 192.168.28.118 * 192.168.28.127 * 192.168.28.84 * 192.168.28.175 * 192.168.28.12 * 192.168.28.56 * 192.168.28.145 * 192.168.28.222 * 192.168.28.6 * 192.168.28.189 * 192.168.28.69 * 192.168.28.174 * 192.168.28.89 * 192.168.28.7 * 192.168.28.57 * 192.168.28.98 * 192.168.28.102 * 192.168.28.18 * 192.168.28.21 * 192.168.28.73 * 192.168.28.178 * 192.168.28.54 * 192.168.28.113 * 192.168.28.87 * 192.168.28.76 * 192.168.28.171 * 192.168.28.156 * 192.168.28.192 * 192.168.28.129 * 192.168.28.190 * 192.168.28.70 * 192.168.28.34 * 192.168.28.132 * 192.168.28.9 * 192.168.28.116 * 192.168.28.140 * 192.168.28.95 * 192.168.28.26 * 192.168.28.62 * 192.168.28.66 * 192.168.28.80 * 192.168.28.3 * 192.168.28.63 * 192.168.28.210 * 192.168.28.143 * 192.168.28.11 * 192.168.28.131 * 192.168.28.130 * 192.168.28.82 * 192.168.28.220 * 192.168.28.117 * 192.168.28.121 * 192.168.28.78 * 192.168.28.24 * 192.168.28.191 * 192.168.28.4 * 192.168.28.32 * 192.168.28.123 * 192.168.28.99 * 192.168.28.22 * 192.168.28.35 * 192.168.28.96 * 192.168.28.37 * 192.168.28.152 * 192.168.28.93 * 192.168.28.209 * 192.168.28.64 * 192.168.28.153 * 192.168.28.101 * 192.168.28.81 * 192.168.28.108 * 192.168.28.23 * 192.168.28.207 * 192.168.28.106 * 192.168.28.239 * 192.168.28.39 * 192.168.28.125 * 192.168.28.151 * 192.168.28.30 * 192.168.28.85 * 192.168.28.155 * 192.168.28.17 * 192.168.28.72 * 192.168.28.10 * 192.168.28.208 * 192.168.28.221 * 192.168.28.86 * 192.168.28.126 * 192.168.28.206 * 192.168.28.74 * 192.168.28.15 * 192.168.28.112 * 192.168.28.90 * 192.168.28.94 * 192.168.28.111 * 192.168.28.154 |

|  |  |
| --- | --- |
| 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 | * 192.168.28.79 * 192.168.28.107 * 192.168.28.36 * 192.168.28.105 * 192.168.28.100 * 192.168.28.59 * 192.168.28.104 * 192.168.28.110 * 192.168.28.97 * 192.168.28.179 * 192.168.28.77 * 192.168.28.118 * 192.168.28.61 * 192.168.28.127 * 192.168.28.84 * 192.168.28.175 * 192.168.28.12 * 192.168.28.56 * 192.168.28.145 * 192.168.28.222 * 192.168.28.6 * 192.168.28.189 * 192.168.28.164 * 192.168.28.69 * 192.168.28.52 * 192.168.28.174 * 192.168.28.89 * 192.168.28.7 * 192.168.28.57 * 192.168.28.98 * 192.168.28.102 * 192.168.28.18 * 192.168.28.21 * 192.168.28.240 * 192.168.28.73 * 192.168.28.238 * 192.168.28.178 * 192.168.28.54 * 192.168.28.113 * 192.168.28.87 * 192.168.28.76 * 192.168.28.133 * 192.168.28.171 * 192.168.28.156 * 192.168.28.192 * 192.168.28.129 * 192.168.28.14 * 192.168.28.167 * 192.168.28.190 * 192.168.28.70 * 192.168.28.1 * 192.168.28.225 * 192.168.28.53 * 192.168.28.34 * 192.168.28.132 * 192.168.28.9 * 192.168.28.234 * 192.168.28.116 * 192.168.28.140 * 192.168.28.95 * 192.168.28.26 * 192.168.28.62 * 192.168.28.8 * 192.168.28.66 * 192.168.28.80 * 192.168.28.3 * 192.168.28.218 * 192.168.28.63 * 192.168.28.210 * 192.168.28.103 * 192.168.28.235 * 192.168.28.248 * 192.168.28.143 * 192.168.28.252 * 192.168.28.5 * 192.168.28.11 * 192.168.28.131 * 192.168.28.130 * 192.168.28.82 * 192.168.28.220 * 192.168.28.13 * 192.168.28.33 * 192.168.28.117 * 192.168.28.121 * 192.168.28.78 * 192.168.28.24 * 192.168.28.191 * 192.168.28.4 * 192.168.28.92 * 192.168.28.32 * 192.168.28.134 * 192.168.28.123 * 192.168.28.99 * 192.168.28.173 * 192.168.28.168 * 192.168.28.22 * 192.168.28.35 * 192.168.28.96 * 192.168.28.37 * 192.168.28.152 * 192.168.28.93 * 192.168.28.209 * 192.168.28.245 * 192.168.28.64 * 192.168.28.153 * 192.168.28.101 * 192.168.28.81 * 192.168.28.108 * 192.168.28.23 * 192.168.28.251 * 192.168.28.207 * 192.168.28.106 * 192.168.28.67 * 192.168.28.239 * 192.168.28.39 * 192.168.28.125 * 192.168.28.151 * 192.168.28.114 * 192.168.28.30 * 192.168.28.85 * 192.168.28.155 * 192.168.28.17 * 192.168.28.72 * 192.168.28.10 * 192.168.28.208 * 192.168.28.221 * 192.168.28.86 * 192.168.28.126 * 192.168.28.206 * 192.168.28.38 * 192.168.28.74 * 192.168.28.15 * 192.168.28.247 * 192.168.28.112 * 192.168.28.90 * 192.168.28.75 * 192.168.28.94 * 192.168.28.111 * 192.168.28.154 * 192.168.28.109 * 192.168.28.161 |

|  |  |
| --- | --- |
| 弱點名稱 | ms08\_067 |
| 弱點敘述 | 攻擊者弱成功利用此弱點，即可能造成使用者電腦受駭。其中TSPY\_GIMMIV.A 惡意程式可能會下載WORM\_GIMMIV.A 蠕蟲，並針對此弱點進行攻擊，而造成使用者系統受駭，導致用戶的帳號密碼、系統資訊等機敏性資料外洩，並可能造成受駭主機的防毒軟體無法執行、運作不正常 |
| 建議措施 | 相關解決方法，請輸入以下網址，https://blog.xuite.net/antivirus/hisecure/23147429-Conficker+%E8%A0%95%E8%9F%B2%E5%88%A9%E7%94%A8%E5%BE%AE%E8%BB%9FMS08-067+%E5%BC%B1%E9%BB%9E%E9%80%B2%E8%A1%8C%E6%94%BB%E6%93%8A%E4%B8%A6%E9%80%8F%E9%81%8E%E7%B6%B2%E8%B7%AF%E9%80%B2%E8%A1%8C%E6%93%B4%E6%95%A3%EF%BC%81 |
| 風險IP |  |

|  |  |
| --- | --- |
| 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 |  |

#### 資料共享風險詳細資訊

* RDP 詳細資訊

|  |  |
| --- | --- |
|  | RDP風險IP |