## 重大風險

### Redis Server Unprotected by Password Authentication

#### 主機IP及服務相對應之埠號

192.168.1.59:6379

#### CVSS分數

7.5

#### 風險敘述

遠端主機上執行的 Redis 伺服器不受密碼驗證保護。遠端攻擊者可加以惡意利用，以取得未經授權的伺服器存取權限。

#### 修補建議

在 redis.conf 設定檔中啟用「requirepass」指示詞。

### SSL Version 2 and 3 Protocol Detection

#### 主機IP及服務相對應之埠號

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

10.0

#### 風險敘述

遠端服務接受使用 SSL 2.0 和/或 SSL 3.0 連線。這些 SSL 版本受到數個密碼編譯瑕疵的影響，包括：  
  
- 具有 CBC 密碼的不安全填補配置。  
  
- 不安全的工作階段重新交涉和恢復配置。  
  
攻擊者可惡意利用這些瑕疵，進行攔截式攻擊或解密受影響服務和用戶端之間的通訊。  
  
雖然 SSL/TLS 可以透過安全的方式選擇通訊協定受支援的最高版本 (因此，只有在用戶端或伺服器支援更好時，才會使用這些版本)，但仍有許多網頁瀏覽器以不安全的方式實作，進而允許攻擊者降級連線 (例如 POODLE 中的連線)。因此，建議完全停用這些通訊協定。  
  
NIST 確定不再接受 SSL 3.0 用於安全通訊。截至 PCI DSS v3.1 中強制執行的日期，任何版本的 SSL 皆不符合 PCI SSC 的「強式密碼編譯」定義。

#### 修補建議

請參閱應用程式的文件，停用 SSL 2.0 和 3.0。  
  
改用 TLS 1.2 (包含核准的加密套件) 或更新版本。

## 高風險

### Microsoft Windows LAN Manager SNMP LanMan Services Disclosure

#### 主機IP及服務相對應之埠號

192.168.1.43:161

#### CVSS分數

7.5

#### 風險敘述

It is possible to obtain the list of LanMan services on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.3.1.1  
  
An attacker may use this information to gain more knowledge about the target host.

#### 修補建議

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

### MongoDB 5.0.x < 5.0.25 / 6.0.x < 6.0.14 / 7.0.x < 7.0.6 Improper Input Validation (SERVER-85263)

#### 主機IP及服務相對應之埠號

192.168.1.59:27017

#### CVSS分數

5.0

#### 風險敘述

The version of MongoDB installed on the remote host is prior to 5.0.25, 6.0.14, or 7.0.6. It is, therefore, affected by a vulnerability as referenced in the SERVER-85263 advisory.  
  
- Improper validation of certain metadata input may result in the server not correctly serialising BSON.  
  
This can be performed pre-authentication and may cause unexpected application behavior including unavailability of serverStatus responses. This issue affects MongoDB Server v7.0 versions prior to 7.0.6, MongoDB Server v6.0 versions prior to 6.0.14 and MongoDB Server v.5.0 versions prior to 5.0.25.  
  
(CVE-2024-3372)  
  
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

#### 修補建議

Upgrade to MongoDB version 5.0.25 / 6.0.14 / 7.0.6 or later.

### SNMP Agent Default Community Name (public)

#### 主機IP及服務相對應之埠號

192.168.1.43:161

#### CVSS分數

7.5

#### 風險敘述

可以獲得遠端 SNMP 伺服器的預設社群名稱。  
  
攻擊者可能會利用此資訊獲得與遠端主機有關的更多資訊，或是變更遠端系統的組態 (若預設社群允許此類修改)。

#### 修補建議

在不使用時停用遠端主機上的 SNMP 服務。  
  
可篩選此連接埠的傳入 UDP 封包，或是變更預設的社群字串。

### SSL Certificate Signed Using Weak Hashing Algorithm

#### 主機IP及服務相對應之埠號

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

5.0

#### 風險敘述

遠端服務使用已利用經密碼編譯的弱式雜湊演算法 (如 MD2、MD4、MD5 或 SHA1) 簽署的 SSL 憑證鏈。已知這些簽章演算法容易受到衝突攻擊影響。攻擊者可加以惡意利用，產生具有相同數位簽章的其他憑證，藉此偽裝成受影響的服務。  
  
請注意，此外掛程式會報告所有透過 SHA-1 簽署且在 2017 年 1 月 1 日之後到期的 SSL 憑證鏈為弱點。做法是依照 Google 的 SHA-1 密碼編譯雜湊演算法逐步淘汰。  
  
請注意，包含在 Nessus CA 資料庫 (known\_CA.inc)中的憑證鏈已遭略過。

#### 修補建議

請聯絡憑證授權單位，要求重新發出 SSL 憑證。

### SSL Medium Strength Cipher Suites Supported (SWEET32)

#### 主機IP及服務相對應之埠號

192.168.1.43:3389

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

5.0

#### 風險敘述

遠端主機支援提供中強度加密的 SSL 密碼。Nessus 將任何使用長度為 64 至 112 位元間的金鑰或使用 3DES 加密套件視為中強度加密。  
  
請注意，如果攻擊者位於同一個實體網路，就更加容易規避中強度加密。

#### 修補建議

重新設定受影響的應用程式，盡可能避免使用中強度加密。

## 中風險

### JQuery 1.2 < 3.5.0 Multiple XSS

#### 主機IP及服務相對應之埠號

192.168.1.244:8080

#### CVSS分數

4.3

#### 風險敘述

根據指令碼中自我報告的版本，遠端 Web 伺服器上託管的 JQuery 為 1.2 或之後版本，或者為 3.5.0 之前的版本。因此受到多個跨網站指令碼弱點影響。  
  
請注意，此外掛程式中提及的弱點不會對 PAN-OS 造成安全性影響，且/或在執行 PAN-OS 版本的裝置上不存在成功惡意利用所需的情況。

#### 修補建議

Upgrade to JQuery version 3.5.0 or later.

### Microsoft Windows LAN Manager SNMP LanMan Users Disclosure

#### 主機IP及服務相對應之埠號

192.168.1.43:161

#### CVSS分數

5.0

#### 風險敘述

It is possible to obtain the list of LanMan users on the remote host by sending SNMP requests with the OID 1.3.6.1.4.1.77.1.2.25.1.1  
  
An attacker may use this information to gain more knowledge about the target host.

#### 修補建議

Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.

### SMB Signing not required

#### 主機IP及服務相對應之埠號

192.168.1.18:445

192.168.1.20:445

192.168.1.5:445

192.168.1.7:445

192.168.30.224:445

192.168.30.229:445

#### CVSS分數

5.0

#### 風險敘述

遠端 SMB 伺服器不需要簽署。未經驗證的遠端攻擊者可惡意利用此弱點，對 SMB 伺服器發動攔截式攻擊。

#### 修補建議

在主機的組態中強制訊息簽署。在 Windows 中，此項目位於原則設定「Microsoft 網路伺服器：數位簽署通訊 (永遠)」中。在 Samba 中，此設定稱為「伺服器簽署」。如需詳細資訊，請參閱「另請參閱」連結。

### SSL Certificate Cannot Be Trusted

#### 主機IP及服務相對應之埠號

192.168.1.43:3389

192.168.1.59:8080

192.168.1.59:8090

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

6.4

#### 風險敘述

無法信任伺服器的 X.509 憑證。此情況可能以三種不同的方式發生，可導致信任鏈損毀，如下所述：  
  
- 首先，可能無法從已知公開憑證授權單位承襲伺服器傳送的憑證鏈結頂端。鏈結的頂端是未經過識別的自我簽署憑證，或缺少將憑證鏈結的頂端連結到已知公開憑證授權單位的中介憑證時，會發生此狀況。  
  
- 第二，憑證鏈結可能包含掃描時無效的憑證。在憑證的其中一個「notBefore」日期之前或憑證的其中一個「notAfter」日期之後進行掃描時，會發生此狀況。  
  
- 第三，憑證鏈結可能包含不符合憑證資訊或無法驗證的簽章。取得錯誤簽章由其發行單位重新簽署的憑證，即可修正錯誤的憑證。由於憑證的發行單位使用 Nessus 不支援或未識別的簽署演算法而無法驗證的簽章。  
  
如果遠端主機是生產環境中的公開主機，鏈結中出現的任何中斷都會導致使用者更難驗證 web 伺服器的真實性和身分。這將造成更容易對遠端主機發動攔截式攻擊。

#### 修補建議

購買或產生適合此伺服器的 SSL 憑證。

### SSL RC4 Cipher Suites Supported (Bar Mitzvah)

#### 主機IP及服務相對應之埠號

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

4.3

#### 風險敘述

遠端主機支援在一個或多個加密套件中使用 RC4。  
  
RC4 加密的似隨機位元組資料流產生程序存有瑕疵，因此多種小偏差被引入資料流中，從而降低了其隨機性。  
  
若純文字遭重複加密 (如 HTTP cookie)，且攻擊者能取得許多 (亦即上千萬) 加密文字，那么攻擊者可以衍生純文字。

#### 修補建議

重新設定受影響的應用程式，如果可以請避免使用 RC4 加密。考慮使用 TLS 1.2，其具有受限於瀏覽器和 Web 伺服器支援的 AES-GCM 套件。

### SSL Self-Signed Certificate

#### 主機IP及服務相對應之埠號

192.168.1.43:3389

192.168.1.59:8080

192.168.1.59:8090

#### CVSS分數

6.4

#### 風險敘述

此服務的 X.509 憑證鏈結並非由已識別的憑證授權單位簽署。如果遠端主機是生產環境中的公用主機，這會造成 SSL 的使用無效，因為任何人都可以對遠端主機發動攔截式攻擊。  
  
請注意，此外掛程式不會檢查以未自我簽署、而是由未識別的憑證授權單位簽署的憑證結束的憑證鏈結。

#### 修補建議

購買或產生適合此伺服器的 SSL 憑證。

### TLS Version 1.0 Protocol Detection

#### 主機IP及服務相對應之埠號

192.168.1.43:3389

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

6.1

#### 風險敘述

遠端服務接受使用 TLS 1.0 加密的連線。TLS 1.0 有幾個加密設計缺陷。現今的 TLS 1.0 實作方式緩解了這些問題，不過，應儘可能使用如 1.2 和 1.3 這種特別針對這些缺陷而設計的較新 TLS 版本。  
  
自 2020 年 3 月 31 日起，未啟用 TLS 1.2 和更新版本的端點將無法再透過主要網頁瀏覽器和主要廠商正常運作。  
  
PCI DSS v3.2 要求必須在 2018 年 6 月 30 日之前完全停用 TLS 1.0，但經確認不受任何已知惡意利用危害的 POS POI 終端機 (及其所連線的 SSL/TLS 終端點) 除外。

#### 修補建議

啟用 TLS 1.2 與 1.3 支援，並停用 TLS 1.0 支援。

### TLS Version 1.1 Deprecated Protocol

#### 主機IP及服務相對應之埠號

192.168.1.43:3389

192.168.30.227:3269

192.168.30.227:636

#### CVSS分數

6.1

#### 風險敘述

遠端服務接受使用 TLS 1.1 加密的連線。TLS 1.1 缺少對目前和建議的加密套件的支援。支援在 MAC 計算之前加密的加密法以及經驗證的加密模式 (如 GCM) 無法搭配 TLS 1.1 使用  
  
自 2020 年 3 月 31 日起，未啟用 TLS 1.2 和更新版本的端點將無法再透過主要網頁瀏覽器和主要廠商正常運作。

#### 修補建議

啟用 TLS 1.2 與/或 1.3 支援，並停用 TLS 1.1 支援。

## 低風險

### ICMP Timestamp Request Remote Date Disclosure

#### 主機IP及服務相對應之埠號

192.168.1.244:0

192.168.1.59:0

192.168.30.224:0

#### CVSS分數

2.1

#### 風險敘述

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.  
  
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

#### 修補建議

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).