張貼日期：2025/06/19

【漏洞預警】趨勢科技旗下 Endpoint Encryption PolicyServer 存在多個重大資安漏洞

- 主旨說明:【漏洞預警】趨勢科技旗下 Endpoint Encryption PolicyServer 存在多個重大資安漏洞

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202506-00000012
  - Trend Micro Endpoint Encryption PolicyServer (TMEE) 是趨勢科技旗下一款為企業提供 Windows 裝置的全碟與可攜式媒體加密，廣泛應用於需遵循資料保護法規的高管控產業中。近日發布重大資安公告修補多項漏洞：
  - CVE-2025-49212CVSS9.8 TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的TMEE安裝執行任意程式碼。
  - CVE-2025-49213CVSS9.8 TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的TMEE安裝執行任意程式碼。
  - CVE-2025-49214CVSS8.8 攻擊者必須先取得目標系統上執行低權限程式碼權限後，允許經過驗證的攻擊者遠端執行程式碼，執行TMEE中的不安全反序列化作業。
  - CVE-2025-49215CVSS8.8 攻擊者必須先取得目標系統上執行低權限程式碼權限後，允許經過驗證的攻擊者使用SQL注入漏洞影響安裝的權限。
  - CVE-2025-49216CVSS9.8 此漏洞允許繞過身分驗證的攻擊者，以管理員身分存取關鍵方法並修改產品配置。
  - CVE-2025-49217CVSS9.8 TMEE 存在不安全的反序列化操作，允許未經身分驗證的遠端攻擊者在受影響的TMEE安裝執行任意程式碼。
- 影響平台:
  - Trend Micro Endpoint Encryption (TMEE) PolicyServer 6.0.0.4013 (不含)之前版本
- 建議措施:
  - 更新 Trend Micro Endpoint Encryption (TMEE) PolicyServer 至 6.0.0.4013 (含)版本
- 參考資料:
  - https://www.twcert.org.tw/tw/cp-169-10186-4abcc-1.html

計算機與通訊中心
網路系統組 敬啟