資訊安全漏洞管理原則

Moxa 致力於嚴謹的產品[i]資安漏洞管理，並提供客戶可靠的產品資訊安全漏洞指引與緩解方法，將產品資訊安全漏洞相關風險降至最低。為此，Moxa 設立產品資安事件應變小組 (Product Security Incident Response Team,以下稱 PSIRT) ，負責處理回報至 Moxa 的產品資訊安全事件與相關產品漏洞通報事宜。Moxa 持續參考國際及業界廣為接受與認定的相關作法與標準[ii]，不斷強化資安漏洞處理程序與回應措施，以積極的態度支持工業網路安全，成為客戶信賴的合作夥伴。

產品資安漏洞管理程序

Moxa 的產品資安漏洞管理程序分為五個階段，每一階段皆具有嚴謹的處理流程與作業。

圖一、資安漏洞管理程序

- 首次事件回應：PSIRT 收到外部針對 Moxa 產品的漏洞回報後，通常將在兩個工作天內對回報者提出的疑慮作出回應。
- 評估與分類：PSIRT 將對回報的產品資安漏洞進行分類與分析，以初步確認該漏洞對 Moxa 產品的影響程度。此階段完成後會提供初步評估結果給漏洞回報者。
- 調查：PSIRT 將與產品開發部門共同協作，確認漏洞的根因 (Root Cause) 及對 Moxa 產品的影響程度與範圍，並進一步針對根因分析出緩解與解決方式。在此階段，PSIRT 與回報者會保持積極的溝通。
- 修復：PSIRT 將與產品開發部門共同協作，進行最終軟/韌體修復方案或緩解措施的開發與驗證。同時，PSIRT 將持續關注相關漏洞訊息的更新以便正確評估漏洞的嚴重性。當開發完整修復方案所需的時間較長，同時漏洞可能造成使用者的高度資安風險時， Moxa 會在最終修復方案完成前，先提供客戶及時的替代緩解措施。
- 揭露：PSIRT 將根據產品資安漏洞的分析結果提供資安通告 (Security Advisory) 。內容包括：漏洞說明、可能受影響的產品與版本列表，以及緩解措施或修復計畫說明。

Moxa PSIRT 與研發團隊透過通用漏洞評分系統 (Common Vulnerability Scoring System, CVSS)及 Moxa 風險漏洞管理模型 (Moxa Risk-based Vulnerability Management Model)，根據安全情境 (Security Context) 、漏洞被利用的可能性以及被利用時可能構成的影響等因素，評估該資安漏洞的潛在風險，並據此決定處理該漏洞之期程。

在確認該漏洞對 Moxa 產品可能的影響後，Moxa 隨即設置專用的測試環境，進一步驗證漏洞的有效性、嚴重性與影響力。必要時將與回報者/資安事件通報組織做進一步溝通。在確定漏洞的根因及其對 Moxa 產品的影響程度及範圍後，Moxa 會進行修復分析，並提供解決方案或緩解措施計畫。

關於產品資安通告的更新與發佈，請參考 Moxa 官網的 Security Advisories 頁面。Moxa 客戶可以通過 (1) 使用 RSS 閱讀器訂閱 Moxa 資安通告或 (2) 建立 Moxa 官網會員帳號並「關注更新」指定產品以獲得該產品最新的產品資安通告。

產品資安問題聯絡窗口

如果您在任何 Moxa 產品中發現可疑的資安漏洞，請立即回報給我們。對 Moxa 而言，及時發現資安漏洞為降低潛在產品資安風險的關鍵。您可透過 PSIRT 電郵信箱向我們回報與 Moxa 產品相關的資安事件，並請使用 Moxa PSIRT 的 PGP 金鑰加密您的訊息與任何佐證附件。

回報產品資安漏洞時，若您的報告包含以下資訊，將能加速我們進行風險評估與提供修復或緩解措施：

1. 產品名稱與型號
2. 軟/韌體版本
3. 重現問題所需的設備及軟體
4. 重現問題的步驟(如果可以，請附上圖片或程式碼)
5. 概念驗證或漏洞利用程式碼
6. 攻擊者可以如何利用此弱點
7. 攻擊的過程之封包側錄
8. 其他您想補充的資訊

- PSIRT 電郵信箱: PSIRT@moxa.com
- 下載 Moxa PGP 金鑰

免責聲明

資訊安全漏洞管理原則各個部分可能會視個案情況而有所變更。我們不保證對任何特定問題做出回應。若使用本文件中包含的資訊或本文件中連結的內容，需由您自行承擔風險。Moxa 保留隨時修改本原則中任何內容的權利，恕不另行通知。如有任何修改，修訂後的文件將公告於 Moxa 官方網站: www.moxa.com 。

---

[i]所指產品適用於 Moxa 所有銷售中的標準產品。至於非標準產品，如訂製品或含有客製化功能的產品則依照特定合約內容進行維護與回應。

[ii] Moxa 參照多項標準，包含:

- 漏洞評鑑結合國際廣為接受與認定的 FIRST (Forum Incident Response Teams) Common Vulnerability Scoring System
- 國際資安組織 FIRST 提出之 PSIRT Services Framework v1.1
- ISO/IEC 29147:2018 Vulnerability Disclosure