VicOne

Driving Automotive Cybersecurity Forward

電動車車隊的隱藏威脅：為什麼車用資安是企業的當務之急

概述

全球運輸產業正在經歷重大轉變，電動車車隊（EV Fleet）在商業和物流領域日益受到青睞。各國政府透過更嚴格的排放法規和獎勵措施，亦加速推動電動車的普及。

全球各地政府正透過嚴格的排放標準和補助計畫來促進車輛轉型。例如，歐盟和美國已推出更嚴格的排放標準，提高內燃機（ICE）車輛的成本，使電動車成為更具吸引力的選擇。印度則設定了宏偉目標，計畫到 2027 年讓 50,000 輛電動公車上路；台灣則是要求到 2030 年，所有市區內的客運公車及政府機關派遣車輛必須全面電動化。

因應政策變化，車隊從內燃機汽車轉向使用電動車，隨著軟體定義汽車（SDV）的發展，新功能也隨之出現。雖然這些進步為車隊管理者帶來許多好處，卻也因網路安全防護不足而增加了風險。我們的汽車威脅情報監測顯示，與車輛相關的網路攻擊在過去四年間激增了 600%，攻擊的主要目標包括電動車充電基礎設施、車上資訊娛樂系統、防盜系統、API 以及連網應用程式。

在政府法規推動電動車車隊普及的同時，企業也必須提高警覺，防範這些轉型帶來的網路安全挑戰。本白皮書將探討電動車車隊數位化與連網技術帶來的關鍵資安風險，並提供最佳實踐建議，協助企業在擁抱綠色永續運輸未來的同時，確保業務營運安全無虞。

車隊營運(Fleet Operations) 的潛在網路安全風險

2022 年，駭客利用 API 漏洞攻擊了俄羅斯一款知名的計程車應用程式，發送大量虛假訂單，將數十輛計程車引導至同一地點，導致莫斯科市區發生大規模交通擁堵，持續了大約一個小時。類似的案例是 2024 年某汽車製造商系統中的一個軟體漏洞暴露了 800,000 輛電動汽車的即時位置數據，讓惡意攻擊者能夠追蹤車輛並存取敏感的駕駛資訊，包括車主的住家地址。

對 EV 車隊的網路攻擊可能導致以下後果：

- **位置數據篡改與隱私風險**：車隊管理系統的數據若遭篡改，可能帶來安全與業務風險。例如，若駭客掌握了車輛的即時位置資訊，可能導致貨物被竊，甚至讓競爭對手得以分析配送路線，影響營運效率。此外，敏感位置資訊外洩將衍生重大隱私問題，使企業面臨監管與合規性問題。根據 VicOne 汽車安全研究團隊研究發現，部分車輛追蹤系統供應商在未加密情況下傳輸數據，這可能讓攻擊者輕易篡改位置資訊。

- **車輛劫持**：攻擊者可能會破壞並入侵車輛的先進車載系統，以遠端控制或竊取車輛來擾亂車隊營運，造成財務與物流損失。在 Pwn2Own Vancouver 2024 資安競賽大會上，研究人員即發現了一個車輛漏洞，該漏洞可能使惡意攻擊者能夠執行任意代碼，導致汽車被竊走或者是關鍵系統遭到未經授權的控制。

- **充電站運作中斷**：對充電基礎設施的攻擊可能導致充電站癱瘓無法運行，讓車輛無法充電，並直接影響車隊的運作效率。在 Pwn2Own Automotive 2025 車用資安競賽大會上，短短三天內就發現

了 23 個電動車充電系統的零日漏洞。從 EV 充電器的漏洞利用，顯見漏洞利用鏈可延伸到充電設備之外，網路犯罪分子可能會將它們用作破壞車輛和連接系統的跳板。

- **勒索軟體攻擊：** 若車隊管理系統遭勒索軟體攻擊，整個營運可能被迫中斷，企業甚至可能需支付高額贖金才能恢復系統以及正常運作。我們的內部研究顯示，2025 年 1 月至 2 月中旬接到通報的汽車勒索軟體事件已經超過 2024 年同期的數量。此外，我們的分析更發現，汽車產業因勒索軟體攻擊造成的財務損失，已從 2022 年的 2.428 億美元飆升到 2023 年的 5.236 億美元。

這些影響涵蓋業務營運、安全性與效率，突顯出數位化電動車車隊所面臨到日益嚴峻的網路安全挑戰。隨著車輛連網技術與自動化程度提升，攻擊面持續擴大，從充電基礎設施到遠端車輛管理系統皆可能成為攻擊目標。

EV Fleet 生態系統的攻擊面

電動車車隊風險從哪裡來呢？在分析整個車隊系統架構時，潛在的攻擊向量可以分類為以下幾個方面：

電動車/商用電動車/三輪電動車

- 未經授權存取車輛控制系統，可能導致遠端接管
- 利用資訊娛樂系統、數位連結儀表板 (DCC)、車載資通系統 (Telematics) 或韌體中的漏洞
- 操縱車載診斷系統（OBD）以篡改車輛性能或安全功能
- 通過無線更新（OTA）機制傳送惡意韌體

充電基礎設施

- 針對充電站的網路攻擊以干擾車隊營運
- 從充電網路攔截數據資料，導致未經授權的能源消耗或是帳單詐欺
- 利用充電器和車輛之間的通信協定漏洞，對車隊安全構成威脅
- 漏洞利用攻擊

行動裝置

- 遭到入侵的車隊管理應用程式，讓攻擊者取得未授權的車輛控制權限
- 針對駕駛員和操作人員的網路釣魚或惡意軟體攻擊，為獲取系統進入及存取的許可權
- 針對行動裝置遠端存取功能的身份驗證機制薄弱

網路架構

- 阻斷服務攻擊 (DoS)，導致車載資通系統或車隊管理系統癱瘓，造成營運中斷、財務損失及安全風險
- 通過操控 GPS、感測器或車輛網路進行篡改與欺騙，用以誤導車隊營運工作人員、更改貨物交付路線，甚至允許執行未經授權的存取，影響安全性和效率

雲端基礎設施

- API 漏洞導致未經授權的數據存取或遠端控制車輛

- 雲端車隊管理平台的漏洞導致敏感的營運數據資料暴露
- 勒索軟體攻擊造成車隊營運中斷
- 通過網路釣魚發起供應鏈攻擊，影響整合在車隊系統中的第三方服務供應商

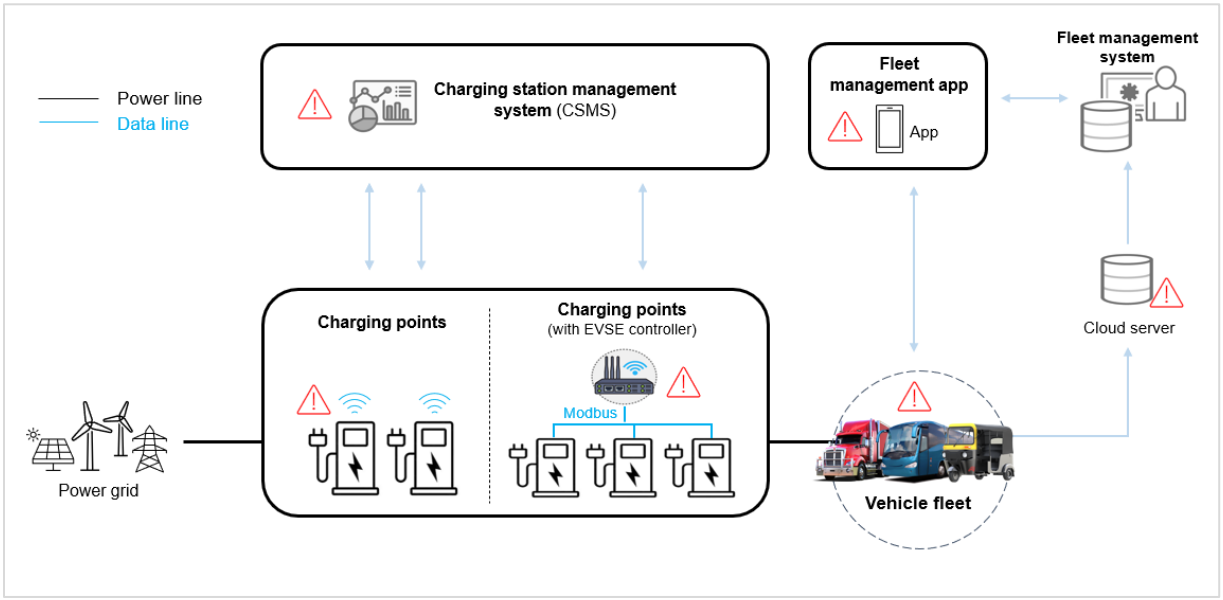

圖 1. 電動車（EV）車隊生態系統中的攻擊面

常見攻擊方法和實際案例

隨著汽車行業的互聯程度越來越高，攻擊者持續利用導航系統、車載資通訊系統、雲端服務與充電基礎設施中的漏洞來發動攻擊。這些攻擊可能會危及車輛安全，擾亂車隊營運，並帶來嚴重的安全風險。以下是一些最為人熟知的攻擊方法和真實案例，顯示電動車車隊生態系統面臨到的持續演變的威脅。

GNSS 欺騙和干擾

2022 年，一名安全研究人員 展示了 惡意行為者如何使用 GNSS（全球導航衛星系統）干擾與欺騙技術來操控或擾亂導航系統。欺騙攻擊的方式是透過發送偽造的 GNSS 信號，使接收器誤以為虛假位置、速度或時間數據為真實資訊。這可能導致車輛偏離預定路線、錯誤的追蹤數據和影響車隊營運。而干擾（jamming）攻擊則是透過強力、持續或「掃頻式」噪聲信號干擾、破話 GNSS，讓接收器無法正確計算位置，從而導致導航失效、自主控制失靈及系統中斷。這些攻擊會帶來嚴重風險，導致誤導性車輛追蹤、營運被迫中斷以及互聯和自動駕駛車輛的潛在安全問題。

ELD 攻擊

電子記錄設備 （ELD） 對於監控車隊活動至關重要，但它們也存在網路安全風險。對 ELD 的主要攻擊可能透過未經授權存取造成車輛系統、車輛控制和安全風險，以及診斷和監控的中斷。在未經授權的控制攻擊中，攻擊者可未經授權以無線方式發送任意 CAN（控制器區域網路）消息，影響某些車輛功能。同時，在韌體操縱攻擊中，攻擊者在 ELD 上安裝惡意韌體，從而能夠更改資料和車輛操作。。

風險類別	特定風險	對車輛的影響
未經授權存取車輛系統	CAN 總線入侵	發送到車輛系統的惡意命令
	ECU 操控	未經授權控制煞車、加速或轉向
車輛控制與安全風險	惡意命令注入	操控車輛功能
	感測器數據篡改	意外反應導致失控
診斷和監測中斷	診斷錯誤	不正確的維護作業
	繞過安全警報	對安全問題的回應能力下降
駕駛員安全和信任	信任受損	駕駛員失去信心
	身體傷害	直接影響駕駛員安全

表 1.ELD 安全性評估

零日漏洞允許在 EV 充電系統上遠端執行惡意程式碼

在 Pwn2Own Automotive 2024 上發現的一個漏洞（CVE-2024-23938）凸顯了影響汽車系統及其支援基礎設施的重大網路安全風險。惡意行為者利用此漏洞注入和執行任意程式碼，從而可能獲得對受影響系統未經授權的控制權。這可能允許他們執行惡意命令或是執行有害軟體，導致充電器和車輛被損壞，甚至造成電網過載。

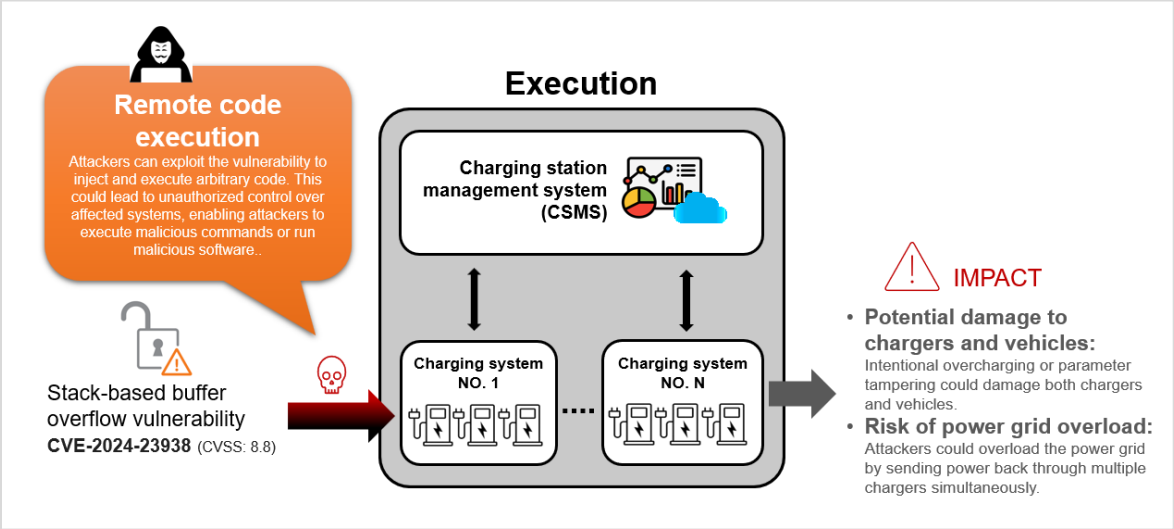

圖 2. 零日漏洞可導致電動車充電系統遭遠端執行惡意程式碼

遠端全面接管車輛：受損的汽車雲端服務 API

2023 年，安全研究人員展示了他們如何通過利用遠端資訊處理系統和 API 中的漏洞來存取各種 OEM 的後端雲端基礎設施。他們發現了一個可供汽車維修廠商直接存取資料的網站，該網站與一家知名汽車品牌的核心員工 LDAP（輕型目錄存取協定）系統皆寫入同一資料庫。在此網站上註冊后，安全研究人員即可直接存取該公司核心員工系統，進而取得敏感資料，其中包括該品牌的 GitHub 內部程式碼，在那裡他們獲取了與客戶車輛通訊的詳細技術資訊。

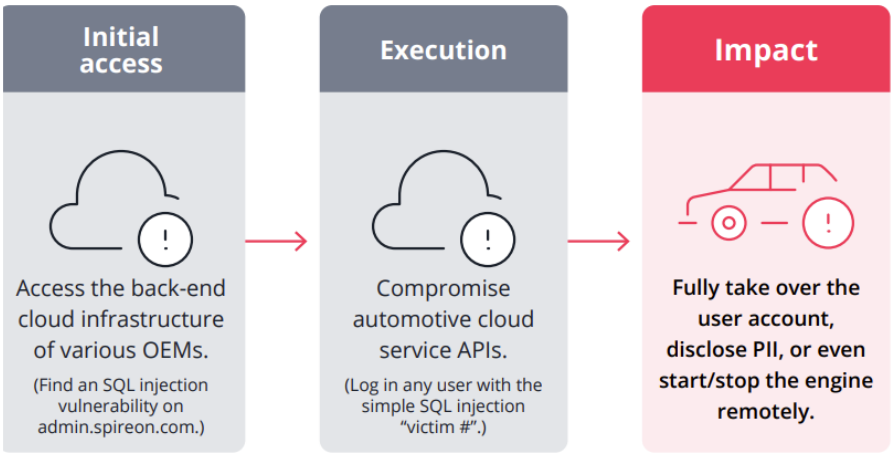

圖 3. 透過入侵汽車雲端服務 API 即可遠端全面接管車輛的攻擊鏈

最佳實踐和安全建議

為了有效降低電動車車隊營運中的網路安全風險，企業組織建議應採取以下措施：

- **持續安全監控：** 蒐集車輛、充電站及相關基礎設施的即時數據，以檢測異常情況並主動回應威脅。例如，五十鈴集團旗下、日本知名商用車 UD Trucks 已經採用了下一代車輛安全營運中心（VSOC）平台。利用情境化的安全洞察與風險分析即早識別新出現的威脅，提高安全監控能力，以符合 UN R155 等標準和法規的監管合規性；該公司亦將威脅情報無縫整合到產品開發生命週期中，持續推動品質改進。
- **可行的威脅情報：** 持續監控深網和暗網的威脅情報，並關聯可能受影響的供應商和元件，以獲取可執行的安全見解。
- **漏洞掃描和管理：**定期對資訊互聯的車載資訊娛樂系統 (IVI)、車載資通系統 (TCU) 及車隊管理平台等進行動態應用安全測試 (DAST)，以預防已知與未知的網路威脅。
- **執行期間的防護：**部署即時監測機制，以偵測異常行為與攻擊，確保運作安全。

- **定期安全更新和 OTA 修補：** 透過部署安全的 OTA 更新機制修補已知漏洞，強化車輛與車隊管理系統的整體安全性。
- **強化加密機制：** 對車輛通訊、數據存儲和 API 端點實施端到端加密，以防止未經授權存取與中間人攻擊（MITM）。
- **強化身份驗證和存取控制：** 對所有車隊管理系統和互聯車輛實施多重身份驗證（MFA）並採用零信任架構，以降低未經授權的遠端存取風險。
- **供應鏈安全：** 監控和驗證整個供應鏈中的軟體和硬體組件，確保第三方供應商符合網路安全標準，降低供應鏈攻擊風險。
- **與汽車網路安全專家合作：** 與專業的車用網路安全服務供應者合作，定期進行滲透測試和安全審計，以發現並修補潛在漏洞。

隨著電動車車隊管理技術的發展，網路安全風險也在持續升高。忽視它們可能會導致重大業務的中斷、財務損失和聲譽受損。為了確保長期穩定性和合規性，車用資安必須視為優先考慮事項。通過加強防禦、持續監控和解決漏洞，企業就能夠保持營運安全和競爭力。

威脅無可避免，但風險是可以管理。現在就是採取行動的時候了。

VicOne

Driving Automotive Cybersecurity Forward