# 資安情資分享

## 2020 年 8 月

# 目錄

# 一、國內網路監視器 DVR 設備資安漏洞，建議用戶立即更新版本


**國內網路監視器 DVR 設備廠商，被發現產品存有多個資安漏洞，遭駭客入侵導致用戶的 DVR 設備產生異常，建議用戶立即更新至最新版本。**

2020 年 1 月，國內爆發大規模網路監視系統駭侵事件，我國多家網路監視器品牌 DVR 主機遭駭侵並植入惡意軟體，導致用戶的 DVR 設備產生異常，業者已於日前釋出新版韌體以修補漏洞。

造成 DVR 設備產生異常的原因係產品的特定函式存有漏洞，因此駭客能透過網址輸入特定參數，取得密碼或是系統檔案，或是針對特定函式進行緩衝區溢位攻擊，取得系統權限。此外，該 DVR 設備的網路限制也存有漏洞，導致駭客可以竄改網路設定檔，對目標裝置注入惡意的系統指令。

遭受攻擊的我國廠商已在官網或經銷商網站、粉絲頁中證實遭到攻擊，並提供緊急處理步驟，包括新版韌體下載、維修服務資源等。

2020 年 2 月，我國廠商在官網釋出新版的 DVR 主機韌體，供用戶更新並修補漏洞。在韌體更新網頁中，提供了多款機種的新版韌體，並強烈建議用戶在更新韌體之後，務必更改預設的管理者帳號與密碼，並使用混合複雜字母、數字與特殊符號的高強度密碼，以免再次發生使用預設帳號密碼，而遭攻擊者輕易進入管理界面的問題。

2019 年在網路上曾有監視錄音工程公司發表一篇文章，直接公開多家廠商 DVR 主機的預設登入用帳號密碼或所謂「萬用工程登入密碼」。有網友指出在這些文件公開之後，多家廠商 DVR 主機就開始陸續傳出被駭災情。

除了更改管理者登入帳密外，資安組織也呼籲用戶修改 DVR 管理界面預設使用的網路埠號，並且在防火牆設定更強大的防護措施。

- 建議採取資安強化措施

1. 建議 DVR 設備的用戶在發現異常時，應儘速與原廠進行聯繫，或是到廠商官網查詢設備的最新資安漏洞訊息，並立即更新至最新版本。更新完成後，也要修改出廠預設的管理員密碼，並同時強化密碼複雜度，以提升設備安全性，以避免發生資安事件而造成損失。
2. 制定公司密碼管理原則，依公司管理機制定期修改密碼，以提高公司設備之安全性。
3. 檢視設備及提供的服務應遵循最小權限原則，減少可能被攻擊的面向。
4. 針對設備之存取進行權限控管，設備本身如有存取控管機制者，可在設備本身進行設定。若無相關存取權限控管，可於前端網路設備如防火牆等，進行相關連線控管機制。

- 資料來源：

1. http://www.icatchinc.com/tw/events_detail.php?id=20200122001
2. http://www.idsmag.com.tw/ids/new_article.asp?ar_id=30954
3. https://portal.cert.tanet.edu.tw/docs/pdf/20190506090530307756179245232.pdf

## 二、數百萬台 Toyota、Hyundai、KIA 汽車面臨無線車鑰遭駭侵者複製的風險


**資安專家指出 Toyota、Hyundai、KIA 等三家車廠使用的無線車鑰系統，其加密演算法存有資安漏洞，駭侵者可輕易取得密鑰資訊，進而竊走車輛。**

比利時 KU Leuven 大學和英國伯明罕大學的研究人員，共同發表研究報告，指出市售多款 Toyota、Hyundai、KIA 車輛使用的無線車鑰加密傳輸協定，存有嚴重漏洞，其加密密鑰可被駭侵者輕易複製。

該研究報告指出，這三大車廠的部分車款，其無線車鑰系統使用的德州儀器 DST80 系統，存有資安漏洞；駭侵者可以利用售價相當便宜的 RFID 掃瞄傳輸裝置，在一定距離內掃瞄無線車鑰，就能取得足夠的資訊；接下來還可以用同一個 RFID 掃瞄傳輸裝置偽裝成真正的無線車鑰，開啟車門並發動車輛。

受該漏洞影響的車款，包括 Toyota 2008 年到 2016 年的 Auris、Camry、Corolla、RAV 4、Yaris、Hiace、Hilux 等，KIA 2011 到 2017 年的 Carens、Soul、Picanto 等，以及 Hyundai 2008 到 2013 年的 i10、i20、IX20、Veloster 等車款。

據 Wired 報導指出，Toyota 已經確認這個資安漏洞確實存在，但該公司認為實務上並不容易使用這個漏洞來竊取車輛，因為必須在很短的距離內才能進行無線車鑰的掃瞄。

值得注意的是，該報告也列入了 Tesla Model S 2018 年款式，不過 Tesla 在去年發布的韌體更新中，已經修補了這個漏洞。

詳細的車款列表，可參考表 1 受影響車輛列表。

表 1、受影響車輛列表

| Make | Period | Model |
|---|---|---|
| Toyota | 2009-2013 | **Auris (2011)** |
| | 2010-2013 | Camry |
| | 2010-2014 | Corolla |
| | 2011-2016 | FJ Cruiser |
| | 2009-2015 | Fortuner |
| | 2010+ | Hiace |
| | 2008-2013 | Highlander |
| | 2009-2015 | **Hilux (2014)** |
| | 2009-2015 | Land Cruiser |
| | 2011-2012 | RAV4 |
| | 2010-2014 | Urban Cruiser |
| | 2011-2013 | Yaris |
| Tesla | 06/2018-07/2019[1] | **Model S (2018)** |

| Make | Period | Model |
|---|---|---|
| Kia | 2012+ | **Ceed (2016)** |
| | 2014 | **Carens (2014)** |
| | 2011-2017 | Rio |
| | 2013+ | Soul |
| | 2013-2015 | Optima |
| | 2011+ | Picanto |
| Hyundai | 2008+ | I10 |
| | 2009+ | I20 |
| | 2009+ | I20 |
| | 2010+ | Veloster |
| | 2016 | **IX20 (2016)** |
| | 2013 | **I40 (2013)** |

資料來源：UNIVERSITY OF BIRMINGHAM AND KU LEUVEN

- 建議採取資安強化措施
  1. 建議受影響車輛列表的車主，應至廠商官網查詢車輛的最新資安漏洞訊息，或是與原車廠進行聯繫，保障車輛安全。
  2. 車主應根據車廠釋出的新版韌體，將韌體更新至最新版本，以修補漏洞，避免車子遭竊。

- 資料來源：
  1. https://tches.iacr.org/index.php/TCHES/article/view/8546/8111
  2. https://www.wired.com/story/hackers-can-clone-millions-of-toyota-hyundai-kia-keys/

# 三、美國多家大型航太製造業者遭勒贖攻擊，拒付贖款後機密內容遭曝光


**多家美國航太製造業者內部重要資料，在遭駭但拒付贖款後被公布在網路上。**

多家美國航太製造業者，包括波音、洛克希德馬丁、SpaceX 等公司，其內部多種重要資料，在遭到駭侵攻擊但拒付贖款之後，資料被公布在網路上。

公布資料的駭侵者據說是在幕後操作 DoppelPaymer 的 Windows 勒贖軟體的駭侵組織；由於上述幾家公司在遭勒贖軟體入侵攻擊後拒付贖金，資料就被公布在網路上。

這批機密度極高的資料中，包括由洛克希德馬丁公司設計製造的軍用裝置的細節，包括反飛彈系統中天線元件的設計規格等。

外洩資料還包括這些公司的各種內部文件，例如支付單據、分析報表、法律文書等，甚至還包括 SpaceX 提供給外包生產廠商的各種資料。

這些資料是駭侵團體攻擊一家名為 Visser Precision 公司所取得的；這家公司是上述幾家大廠的外包廠商。駭侵者駭入 Visser Precision 的電腦，將這批重要檔案加密，並要求數千萬美元的贖金，但遭到拒付。駭侵者便將部分資料公開在網路上作為報復手段。

這並非 DoppelPaymer 駭侵組織第一次公布受害者的資料，該駭侵組織網站，經常貼出許多拒付贖款者所屬的資料，做為恫嚇其他受害者的手段；在駭侵者威脅公開資料時是否支付贖金，即使在資安專家之間，也有各種不同意見。有人認為無論如何都不該助長勒贖攻擊，有些人則認為如果資料過於敏感，支付贖金也是可以考慮的選項。

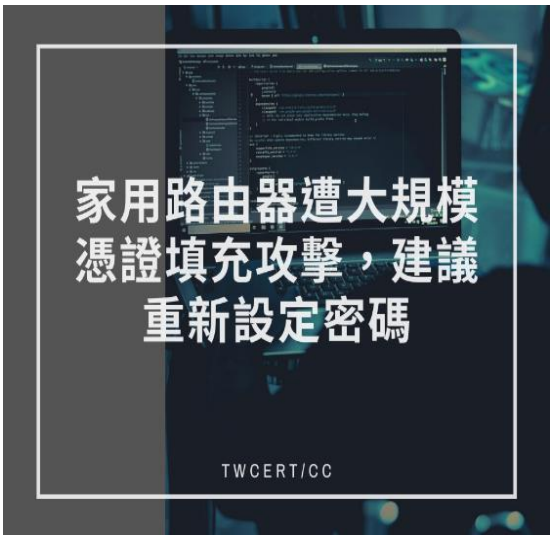
但無論如何，製造業者都應加強資安防護強度，並提高從業人員的資安意識，才能從根本避免愈來愈猖獗的勒贖攻擊事件。

- 建議採取資安強化措施

1. 建議定期將重要資料進行備份。
2. 不隨意開啟不明寄件人寄送的郵件，在未確認寄件人身分或是針對標題及內容可疑的信件，不隨意點擊或下載任何信件中的連結與夾帶附件。不進入可疑或不安全的網站，必須確認網址的正確性，可使用網址識別套件或直接手動鍵入網址，以防止遭駭客入侵，被植入惡意軟體而造成損失。
3. 應定期更新作業系統版本以及軟體或應用程式版本，安裝防毒軟體與防火牆，確保設備軟體處於最新版本。
4. 建議企業進行內部教育訓練，加強資安宣導，提升員工資安意識。
5. 及時發現中了勒索軟體的當下，建議立即將電腦關機，中斷網路連線、拔除實體網路線及 USB 裝置，將受害主機進行隔離。
6. 參考 TWCERT/CC 官網(https://www.twcert.org.tw/tw/lp-22-1-2-20.html)提供之勒索病毒解鎖服務，參考已被解鎖勒索軟體之解鎖工具。

- 資料來源：
  1. https://www.theregister.co.uk/2020/04/10/lockheed_martin_spacex_ransomware_leak/
  2. https://www.malwarebytes.com/ransomware/
  3. https://www.ithome.com.tw/tech/101366
  4. https://blog.trendmicro.com.tw/?p=18070

## 四、家用路由器遭大規模憑證填充攻擊，建議重新設定密碼




**資安專家指出，自 2020 年 3 月起，全球至少有 1200 台 Linksys 家用無線路由器遭到駭侵者以「憑證填充」攻擊得逞；Linksys 鎖定受害用戶的網路管理頁面帳號，以避免遭駭侵者進一步利用。**

資安專家指出，自 2020 年 3 月起全球至少發現有 1200 台 Linksys 家用無線路由器，遭到駭侵者以「憑證填充」（credential-stuffing）攻擊得逞。

駭侵者以大量試誤的方式，與網路上取得的已外洩帳密檔案比對，找到受害用戶的路由器管理者可登入帳密後，接著就會修改路由器的 DNS 設定，導致用戶的網路瀏覽封包被挾持並轉向到惡意網站。

駭侵者攻擊的登入帳密，主要是 Linksys Smart WiFi App 服務的登入資訊；用戶可透過此服務管理自己的 Linksys 路由器設備。一但駭侵者取得此服務的帳密，就可以將用戶導向下載安裝一個稱為 Oski infostealer 的惡意軟體，進一步竊取受害者電腦中的各種機敏資訊。

駭侵者主要鎖定一些熱門網域進行 DNS 挾持，例如 Disney.com、Reddit Blog.com、AWS.amazon.com、Cox.net、Washington.edu 等。用戶進入這些網站時，會被導向到一個假冒的武漢肺炎病毒訊息頁面，如果按下畫面中的按鈕，就會被安裝 Oski infostealer 惡意軟體。

為了遏止這波攻擊，Linksys 自 2020 年 4 月起鎖定所有 Linksys Smart Wi Fi app 用戶的網路管理頁面帳號，並要求用戶重新設定密碼，以避免遭駭侵者進一步利用。

- 建議採取資安強化措施
  1. 建議立即重新設定應用程式的密碼，並定期更換密碼。
  2. 建議使用 12 個字元以上，且為英文、數字與符號混合的密碼，應避免多個系統、網站及應用程式等服務皆使用同一組密碼。
  3. 定期進行應用程式漏洞更新，安裝防毒軟體與防火牆，確保系統、設備與應用程式處於最新版本，避免受到駭客攻擊而造成損失。

- 資料來源：
  1. https://www.linksys.com/us/support-article?articleNum=317063
  2. https://www.linksys.com/us/support-article/?articleNum=246427
  3. https://threatpost.com/attacks-on-linksys-routers-trigger-mass-password-reset/154914/

## 五、國內能源石化與資通產業連續遭駭侵攻擊


**國內多家企業連續傳出遭惡意軟體攻擊事件，疑似駭侵團體發動目標式勒索病毒。**

國內石化能源產業與資訊通訊製造業者等多家企業，傳出連續遭駭侵者以勒贖軟體攻擊事件，造成營運及商譽損失。

首先是一間石化能源產業傳出遭到勒贖軟體攻擊，包括官方網站、營業據點的部分系統，以及部分服務遭到阻斷無法使用；經緊急斷網處理並且啟動備份回復機制後，其官網與大多數營業據點均已恢復正常營運。

隔日，另一間石化能源產業也傳出遭駭侵攻擊事件，發現公司部分電腦設備出現異常；該公司關閉所有電腦並且斷網進行內部清查，於當天逐漸恢復正常，而其營業據點則仍維持正常運作。

同日一間屬於資通產業的企業也傳出災情，旗下某廠的部分伺服器亦遭勒贖軟體駭侵攻擊；該公司同樣採取斷網隔離作業，並回復受損資料，整體損失與對生產作業的影響有限。

遭受駭侵攻擊的石化能源產業，若屬於資通安全法中指定的關鍵基礎設施，在確認遭駭侵攻擊後，都已立即通報資安事件，政府也啟動相關的調查程序。

- 建議採取資安強化措施

1. 檢視 AD(Active Directory) 伺服器權限及帳密，避免駭客入侵電腦後，設定群組原則，導致勒索病毒檔案被下載並在受影響網域內的電腦上執行。
2. 提高資安警覺，不開啟標題及內容可疑或聳動的電子郵件，不點擊其提供的任何連結與附加檔案，收到電子郵件的當下務必先確認寄件人的身分。
3. 提防進入釣魚網站，即使看起來像官網也要確認網址的正確性，進到可疑網站不輸入個資與金融資訊，建議可以手動鍵入網址或是搭配網址識別套件防範釣魚網站。
4. 避免在公司使用私人的外接硬碟設備，以免受感染的設備擴大感染公司的所有系統設備。
5. 企業內部網路建議可藉由分段隔離來減少損害程度、提升各網段間的安全性，並定期將資料備份以減少損失。
6. 落實資安宣導，定期舉辦資安教育訓練及社交工程演練，提高員工資安意識。
7. 安裝防毒軟體及防火牆，定期更新軟體、作業系統與應用程式，防止駭客利用資安漏洞進行駭侵攻擊。
8. 定期多重備份檔案於不同設備，並異地儲存一個備份。

- 資料來源：

1. https://www.cpc.com.tw/News_Content.aspx?n=28&sms=8920&s=4947
2. https://blog.trendmicro.com.tw/?p=64227
3. https://www.twcert.org.tw/tw/cp-104-3600-a5ce6-1.html
4. https://www.us-cert.gov/ncas/tips/ST04-014

5. https://www.nomoreransom.org/zht_Hant/index.html
6. https://www.bnext.com.tw/article/57547/cpc-hack-ransomware
7. https://www.netadmin.com.tw/netadmin/zh-tw/viewpoint/0037B4A129E44701B19DE38807050098

# 六、日本與歐洲多國製造業最近大舉遭駭，尤以能源產業為甚


**資安廠商指出，日本和歐洲多個國家的製造業業者，遭到手法十分複雜成熟的駭侵攻擊，而且攻擊所使用的惡意軟體，愈來愈難以偵測。**

資安廠商卡巴斯基發表研究報告，指出該公司觀測到日本和歐洲多個國家的製造業業者，最近開始遭到手法十分複雜成熟的駭侵攻擊；而且攻擊所使用的手法與惡意軟體，愈來愈難以偵測。

卡巴斯基說，自 2020 年 5 月初開始，發現日本、德國、英國和義大利的多家重要工業設備製造業者和針對製造業者開發軟體的部分公司，陸續遭到駭侵團體鎖定攻擊。

報告指出，在遭駭的業者當中，駭侵者特別著重在能源產業的攻擊；雖然公司的防毒防駭服務已成功阻擋一些攻擊活動，但目前不知駭侵者的攻擊目的為何。

卡巴斯基指出，駭侵者主要的攻擊目標為這些企業的 IT 架構，而非營運或製造節點（OT）；攻擊的目標以竊取系統登入資訊為主。

在卡巴斯基攔截到的攻擊行為中，典型的攻擊樣態仍以釣魚郵件為開始；駭侵者針對攻擊對象發送以該國語言編寫的釣魚郵件，並在確定被駭主機作業系統的語言與釣魚信件一致後，才會展開下一階段的攻擊。

釣魚郵件中含有微軟 Office 文件檔案，內含惡意巨集程式碼；當受害者開啟文件，該巨集就會執行一個 PowerShell 指令檔，並且下載內含進一步攻擊指令的圖片。接著惡意軟體會解開圖片內含的惡意程式碼，產生另一個 PowerShell 指令檔，並且執行著名的密碼竊取軟體 Mimikatz。也因如此多重的手法，造成其攻擊偵測難度提升。

- 建議採取資安強化措施
  1. 應多加防範釣魚郵件，對可疑或聳動標題的電子郵件保有警覺心，收到陌生寄件者寄來的郵件，應使用其他管道加以查證對方身分，不隨意開啟電子郵件，也不點擊郵件內的任何附件、圖片與超連結等。
  2. 調整電子郵件設定的設定，開啟純文字模式、取消預覽功能。
  3. 對 Microsoft Office 文件之巨集功能予以限制或停用。
  4. 安裝防毒軟體及防火牆，確保防毒軟體保持最新狀態，並配合廠商發行的安全性修補程式，定期更新電腦系統、軟體與設備等，以修補資安漏洞。

- 資料來源：
  1. https://www.securityweek.com/industrial-suppliers-japan-europe-targeted-sophisticated-attacks
  2. https://www.ithome.com.tw/news/112744
  3. https://docs.microsoft.com/zh-tw/windows/security/threat-protection/intelligence/macro-malware。

# 七、國內網通設備廠商修復存於家用路由器的嚴重資安漏洞


**國內網通設備廠商修復存於家用路由器的部份資安漏洞，建議仍在使用不支援安全性更新的網通設備產品用戶，應考慮更換並升級至最新版本軟硬體產品組合。**

資安廠商 Palo Alto 網路公司的資安研究團隊 Unit 42，公布六個台灣網通設備廠商家用路由器 DIR-865L 的嚴重資安漏洞；除了這款路由器外，其他採用相同程式碼的路由器亦可能出現相同的漏洞。

這六個漏洞分列如下：

CVE-2020-13782：指令中的特殊元素處理不當，可讓駭侵者植入指令

CVE-2020-13786：跨站請求偽造（CSRF）漏洞

CVE-2020-13785：不適當的加密強度

CVE-2020-13784：可預測的亂數產生器

CVE-2020-13783：以明文儲存機敏資訊

CVE-2020-13787：以明文傳輸機敏資訊

這些漏洞本身的危險程度評級，從 7.5 分的「高等級」到 9.8 分的「嚴重」等級，然而資安專家指出，當駭侵者組合利用這些漏洞時，就會增加駭侵風險。

舉例來說，駭侵者可以先利用明文傳輸與儲存機敏資訊的漏洞，設法取得工作階段的 cookie，然後以此存取管理者權限的各項資源，例如內網的檔案分享服務，並藉以植入更多的惡意軟體程式碼，竊取用戶的各種檔案，任意刪改檔案內容，甚至更可把遭駭路由器當做發動 DDoS 攻擊的僵屍網路節點。

該產品公司在接獲通報後，透過發行 beta 版本韌體的方式，修復了其中三個漏洞；該公司在聲明中指出，DIR-865L 是相當老舊的路由器產品，於 2016 年 2 月 1 日就已結束後續的產品支援，所以未來也不會繼續提供支援。

- 建議採取資安強化措施

建議使用老舊且已不支援安全性更新的網通產品用戶，應考慮升級至最新版本的軟硬體產品組合，並維持產品的軟硬體與系統皆處於最新狀態，避免因為無法取得原廠支援而造成資安損失。

- CVE 編號：CVE-2020-13782~13787
- 影響產品 / 版本：D-Link DIR-865L
- 解決方案：使用廠商提供的部分漏洞修補程式進行更新，或是升級至最新的軟硬體產品組合

- 資料來源：

1. https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174
2. https://unit42.paloaltonetworks.com/6-new-d-link-vulnerabilities-found-on-home-routers/
3. https://www.cyberscoop.com/d-link-home-routers-vulnerabilities-palo-alto-networks/

## 八、駭客利用 BadPower 漏洞，鎖定快速充電器進行攻擊


**資安廠商發現專門鎖定快速充電器的攻擊手法，可能會造成設備起火事故。**

國外的資安研究團隊發現，部分快速充電器產品存在安全問題 BadPower。利用此資安漏洞，駭客能鎖定各種電子設備的快速充電器進行攻擊，可能會造成設備中的零組件燒燬，甚至引起火災事故。

一般來說，市售的快速充電器，和一般充電器看起來差別不大，主要差別在於控制充電速度與電量的韌體程式；設備韌體會和被充電裝置進行溝通，以決定要以多大的電壓或電流進行充電。

利用 BadPower 漏洞的攻擊手法，會提供超過充電裝置額定電壓電流的供電，導致被充電設備的損壞、高溫，甚至發生火災事故。

該資安團隊在報告中指出，某些廠商之產品在資料通道中設有可讀寫充電器韌體程式碼的進入點，要存取這些進入點時，卻沒有足夠安全的認證程序，或是其快充通訊協定內存有可破壞韌體程式碼的漏洞，駭客便是利用這些漏洞進行攻擊。

該資安團隊針對市售 35 款快充設備進行測試，發現 8 個品牌的產品，共 18 款設備存有 BadPower 漏洞問題；針對快速充電器控制晶片廠商調查，發現在 34 家晶片廠中，有 18 家的快充晶片產品可透過各種方式更新韌體；廠

商如果沒有做好相關資安防護，其充電器就可能存有 BadPower 漏洞，並遭到駭客攻擊。

- 建議採取資安強化措施
  1. 根據廠商發布之安全性更新，將充電設備的韌體更新至最新版本。
  2. 建議用戶不要使用 Type-C 轉接其他 USB 傳輸線為不支援快速充電的設備充電，也不建議將快速充電器借給他人使用，以免發生電力過載造成設備損壞。
  3. 建議廠商針對充電器韌體之程式碼進行安全性檢查，並將透過 USB 更新韌體的方式進行嚴格的驗證，防止駭客利用資安漏洞進行攻擊。

- 資料來源：
  1. https://xlab.tencent.com/cn/2020/07/16/badpower/
  2. https://www.zdnet.com/article/badpower-attack-corrupts-fast-chargers-to-melt-or-set-your-device-on-fire/

**台灣電腦網路危機處理暨協調中心**
**(Taiwan Computer Emergency Response Team / Coordination Center)**

服務電話：**0800-885-066**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw/**

痞客邦：**https://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc/**

Instagram：**https://www.instagram.com/twcertcc/**

Twitter：**@TWCERTCC**