



TWCERT/CC 資安情資電子報

TWCERT/CC 資安情資電子報

2024 年 8 月份

2024 年 8 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 4 章節：

第1章、封面故事：本月TWCERT/CC所發布之資安情資中，官網點閱次數最高之情資列為本月份封面故事。

第2章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇可能包含資訊安全宣導、資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟硬體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第3章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第4章、TVN漏洞公告：TWCERT/CC為CVE編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明本月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN)平台其CVSS 3分數為8.8以上之漏洞。

目錄

內容

目錄 II

第 1 章、封面故事.....	1
網路攝影機存在高風險漏洞，可能被用來傳播惡意軟體.....	1
第 2 章、國內外重要資安事件.....	3
2.1 新興應用資安.....	3
2.1.1 Sitting Ducks 對上百萬個網域擁有者造成嚴重威脅.....	3
2.2 國際政府組織資安資訊.....	7
2.2.1 美國宣布禁售卡巴斯基軟體產品.....	7
2.3 社群媒體資安近況.....	9
2.3.1 WordPress 網站爆出嚴重漏洞，影響超過 10 萬個以上的網站.....	9
2.4 軟硬體漏洞資訊.....	11
2.4.1 Avtech 攝影機存在高風險安全漏洞.....	11
2.4.2 Microsoft 作業系統存在高風險安全漏洞.....	12
第 3 章、資安研討會及活動.....	14
第 4 章、TVN 漏洞公告.....	23
編輯：TWCERT/CC 團隊.....	25

第 1 章、封面故事

網路攝影機存在高風險漏洞，可能被用來傳播惡意軟體



美國網際安全暨基礎設施安全局（CISA）日前發布警告，指出由陞泰科技（Avetech Security）製造的網路攝影機存在高風險命令注入漏洞。由於該漏洞尚未修補，且已遭利用攻擊，CISA建議用戶立即採取相關防護措施，以確保系統安全。

該漏洞編號為CVE-2024-7029（CVSS 3.x分數為8.8），允許攻擊者在無需密碼或身份驗證的情況下，可以管理者身份遠端向攝影機注入並執行指令。受影響的設備包括特定韌體版本的AVM1203 IP攝影機。

陞泰科技近期針對本次漏洞發表聲明，指出AVM1230為停產近七年的產品，並表示後續將評估是否釋出修補軟體或提供替代方案。此外，該公司已對目前產品線進行全面檢測，確認目前銷售的機種已經採取相關處理措施與解決方案，確認銷售機種韌體不存在本次漏洞。

CISA指出，此漏洞由Akamai通報，並經第三方組織確認特定產品及韌體存在問題。Akamai研究人員在2024年3月就已發現針對該漏洞進行探測的紀錄，並在分析蜜罐日誌時確認本次漏洞。漏洞存在於文件 /cgi-bin/supervisor/Factory.cgi 的「亮度」功能中，利用此漏洞可使攻擊者在目標系統上遠端執行程式碼。目前，該漏洞已被用來傳播惡意軟體，該惡意軟體疑似是Mirai變種。

由於該漏洞的產品廣泛使用於全球，包括商業設施、醫療保健、金融服務和交通運輸等關鍵基礎設施領域。在廠商尚未釋出修復更新前，CISA建議用戶透過防火牆或相關防護設備限制網際網路的IP存取網路攝影機並與企業內部網路隔離，若有遠端存取的需求，僅開放VPN或特定IP來源等連線方式。

- 資料來源：
 1. <https://nvd.nist.gov/vuln/detail/CVE-2024-7029>
 2. <https://www.cisa.gov/news-events/ics-advisories/icsa-24-214-07>
 3. <https://www.securityweek.com/cisa-warns-of-avtech-camera-vulnerability-exploited-in-wild/>

第 2 章、國內外重要資安事件

2.1 新興應用資安

2.1.1 Sitting Ducks 對上百萬個網域擁有者造成嚴重威脅



Infoblox和Eclypsium的研究人員發現一種網域名稱劫持攻擊，取名為「Sitting Ducks」，有超過百萬個網域易遭受此攻擊，且目前觀察到有數十個與俄羅斯相關的攻擊者正在利用此種攻擊。

Infoblox 和 Eclypsium 的研究人員發現 DNS 存在一種攻擊媒介，且有十多個與俄羅斯有關的攻擊者正在利用此種媒介進行攻擊，這是一種網域名稱劫持，研究人員給其名稱：Sitting Ducks。網域名稱系統(Domain Name System, DNS)是用以將網域名稱與IP連結，網域名稱是為了讓人更好記憶網站，但電腦裝置之間的通訊是透過IP來傳輸，因此透過DNS將網域轉為IP位址，這樣瀏覽器才能載入網站。

過去存在很多種針對DNS進行網域劫持，可讓攻擊者去執行惡意軟體傳播、網路釣魚、品牌冒充及資料外洩，而從2019年以來至

今，Eclipsium 的研究人員認為超過 3 萬個網域被 **Sitting Ducks** 攻擊劫持，且當前有超過百萬個網域都有遭受此攻擊的風險。

Sitting Ducks 攻擊的特性為易於執行攻擊且難以偵測，但可以完全被預防。**Sitting Ducks** 攻擊是攻擊者去劫持目前已經註冊的網域，這些網域註冊在公開具權威性的 DNS 服務供應商或網頁主機供應商，而一旦攻擊者劫持網域，就可以假藉合法者的身分來進行任何惡意活動，如散播惡意程式、寄送釣魚信等。

由於 **Sitting Ducks** 攻擊並不需要攻擊者註冊網域名稱，故而跟常見的 DNS 劫持攻擊有根本的不同。**Sitting Ducks** 攻擊的核心是網域名稱註冊商的錯誤配置和 DNS 提供者的預防不充分所造成。

以下幾種情況可能會發生 **Sitting Ducks** 攻擊：

- 註冊的網域解析使用其他家 DNS 供應商，也就是使用 DNS 委派(即 DNS 伺服器將部分網域解析作業委託其他 DNS 伺服器執行)
- DNS 委派異常，意即接受委派的 DNS 伺服器上並沒有該註冊網域資料，因此無法提供 DNS 查詢。
- DNS 服務供應商設定錯誤，攻擊者可與 DNS 服務供應商聲明其擁有受害者網域名稱並設定 DNS 紀錄，而不需證明其為網域名稱註冊處的對應有效使用者。

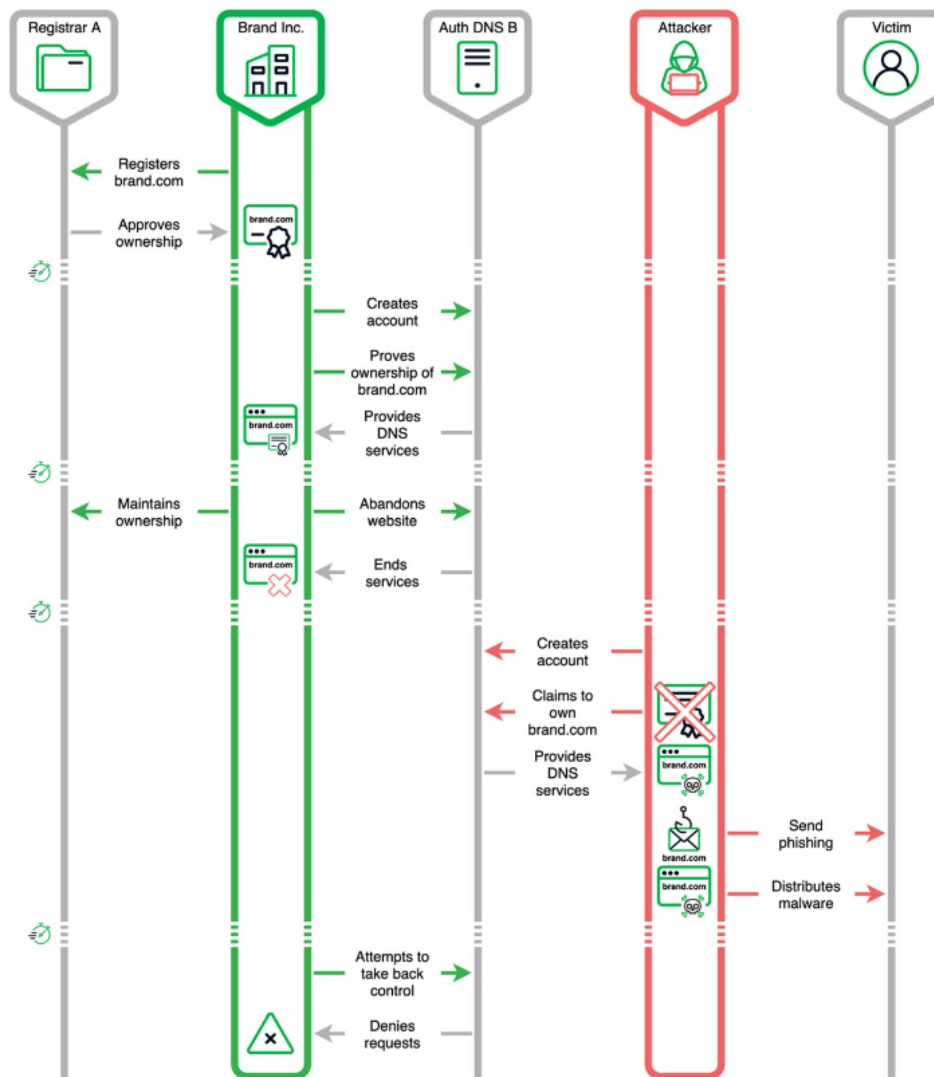
故而促成此攻擊的主要因素就是 DNS 委派上的問題，同時 DNS 服務供應商存在錯誤的設置。

Infoblox 研究人員表示其觀察約十幾個 DNS 服務供應商，發現此攻擊被廣泛利用，尤其以俄羅斯相關犯罪者最為常見，每天有數百個網域被劫持。

圖1說明 **Sitting Ducks** 攻擊的常見流程，主要攻擊過程為受害者跟網域供應商 Registrar A 註冊網域 brand.com，並交由 DNS 服務供應

商 Auth DNS B 做解析

而一段時間後，受害者暫時不再需要使用網域 brand.com，但仍透過Registrar A 保有網域的擁有權，但這時 Auth DNS B 解析服務已過期，這時攻擊者跟 DNS 服務供應商 Auth DNS B 聲稱擁有網域 brand.com 的擁有權，並設置 DNS 解析紀錄，來將該網站解析到攻擊者的惡意網站，此時攻擊者就可以假冒受害者的身分來對其他人發送釣魚郵件或散播惡意程式，這時受害者嘗試跟DNS服務供應商 Auth DNS B聲稱擁有網域 brand.com的擁有權，會遭到拒絕。



圖片取自：<https://blogs.infoblox.com/threat-intelligence/who->

knew-domain-hijacking-is-so-easy/

Sitting Ducks 攻擊是可以被預防的，透過上圖說明可知它的存在成因源自網域名稱和 DNS 紀錄管理上的缺陷，如果網域註冊商跟 DNS 服務供應商是同一家單位則不存在此問題，而如果是不同單位，只要確實做好管理就可以預防攻擊發生

過去也有這次的攻擊事件探討跟發生：

- 此次攻擊最早一次被提及是 2016 年由作者 Matthew Bryant 寫的文章「孤立的網路-透過 DNS 漏洞接管 12 萬個網域」
- 2019年時，攻擊者透過此攻擊濫用了 GoDaddy.com 的弱點發送大量的垃圾郵件

建議網域持有者可以執行以下操作：

- 檢查自己的網域註冊服務商跟DNS 服務供應商是否為同一個提供者，如果是的話則不會受此攻擊影響。
- 檢查自己的網域和子網域是否將網域名稱解析委派給已經過期或無效的服務供應商，若是，請更新資訊以避免受此攻擊影響

諮詢自己的DNS服務供應商是否對此類攻擊已有緩解措施，如果 DNS 服務供應商已經有緩解措施則不必擔心此類攻擊。

- 資料來源：
 1. ['Sitting Ducks' Attacks Create Hijacking Threat for Domain Name Owners](#)
 2. [Who Knew? Domain Hijacking Is So Easy](#)
 3. [Ducks Now Sitting \(DNS\): Internet Infrastructure Insecurity](#)
 4. [The Orphaned Internet – Taking Over 120K Domains via a DNS Vulnerability in AWS, Google Cloud, Racks](#)
 5. [Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com](#)

2.2 國際政府組織資安資訊

2.2.1 美國宣布禁售卡巴斯基軟體產品



美國於2024年7月20日開始禁止資安軟體公司卡巴斯基 (Kaspersky) 在美國銷售網路安全產品及防毒軟體，此項禁令為美國商務部工業及安全局(Bureau of Industry and Security, BIS)於2024年6月20日宣布之裁決結果 (Final Determination)，主要因為該公司產品影響美國國家安全，自2024年9月29日起，卡巴斯基也將被禁止提供相關產品更新，惟未涵蓋卡巴斯基所提供的威脅情報產品/服務、安全培訓產品/服務、顧問與諮詢服務。

卡巴斯基(Kaspersky)是一家全球知名的網路安全公司，總部位於俄羅斯，成立於1997年。由尤金·卡巴斯基(Eugene Kaspersky)創立，該公司專注於提供全面的網路安全解決方案，包括防毒軟體、防火牆等。卡巴斯基的產品服務範圍涵蓋個人、小型企業、大型企業及政府機關，以其高效的威脅檢測和防護技術著稱。公司致力於保護

用戶免受各種網路威脅，並在全球擁有廣大的客戶。

美國工業及安全局針對卡巴斯基軟體對於國家安全構成不當或不可接受的風險原則提出理由如下：

1. 卡巴斯基受到俄羅斯政府的管轄、控制或指揮，可能導致利用卡巴斯基防毒軟體存取電子設備之敏感資訊。
2. 卡巴斯基可透過提供網路安全和防毒軟體，對客戶資訊擁有廣泛的存取與管理權限，因此卡巴斯基的員工可能將美國客戶的資料轉移至俄羅斯。
3. 卡巴斯基可藉由安裝產品在美國客戶設備上之名義，安裝惡意軟體或阻止關鍵更新，使美國客戶和關鍵基礎設施容易受到惡意軟體利用和威脅。
4. 卡巴斯基的軟體產品可透過轉售，將其網路安全或防毒軟體整合到其他第三方產品，將會導致第三方交易中，因軟體原始碼未知而增加卡巴斯基軟體無意間被引入用戶的設備或網路。

此次禁令導致卡巴斯基多項產品受到影響，美國政府允許企業和用戶有一段時間可以尋找替代方案，在2024年9月29日之前仍可更新卡巴斯基的軟體服務。

值得注意的是，該禁令並未涵蓋卡巴斯基所提供的威脅情報產品/服務、安全培訓產品/服務、顧問與諮詢服務。因此，美國組織仍可與卡巴斯基進行教育性質的服務。

● 資料來源：

1. <https://thehackernews.com/2024/06/us-bans-kaspersky-software-citing.htm>

2.3 社群媒體資安近況

2.3.1 WordPress 網站爆出嚴重漏洞，影響超過 10 萬個以上的網站



GiveWP是一個WordPress 網站捐贈Plugin，可以讓網站輕鬆接受來自世界各地的捐贈，近期遭揭露重大資安漏洞(CVE-2024-5932)，可以讓駭客遠端執行任意程式碼且不需要任何身分認證，並能刪除所有檔案，建議使用者應更新至3.14.2版本。

WordPress 此次的漏洞是出現在 GiveWP Plugin，漏洞編號為 CVE-2024-5932，此漏洞在通用漏洞評分系統 (CVSS) 的分數為 10.0 (滿分)，代表了漏洞的嚴重性極高。

此漏洞為PHP物件注入(PHP Object Injection)，主要在 GiveWP Plugin 的 give_title 參數上，可透過注入特殊的PHP物件來觸發反序列化，而該物件跟 Plugin 裡面現有的POP 面向屬性編程鏈結合，成為遠端程式碼執行 (RCE)，也就是攻擊者可不經身份驗證，就可完全控制受漏洞影響的WordPress網站。

序列化是指可將複雜的資料轉換後做儲存，反序列化即是將序

列化後的資料轉換回原本的模樣，如底下是一個 PHP 序列化資料的範例

```
a:2:{s:12:"productPrice";s:5:"11111";s:7:"price";i:10;}
```

PHP 程式碼基本都是物件導向的，其中程式碼被組成「類別」，類別為包含有變數(稱為屬性)和函數(稱為方法)的模板，程式透過類別來創建物件，從而產生可重複使用和維護的程式碼，若Plugin 在沒有清理乾淨的情況下，反序列化使用者輸入的資料，則可能讓攻擊者注入惡意的內容，使其在反序列化的時候變成 PHP 物件，若反序列化出來的物件存在魔法方法 (Magic Method)時，可能會導致惡意的攻擊行為。

魔法方法(Magic Method)是類別中的特殊函數，用以定義某些事件發生時要執行的行為，如不需要物件時要如何清理、創建物件時要初始化執行的事情等。

此漏洞為資安研究員 villu164 透過Wordfence Bug漏洞賞金計畫發現並提出研究報告，鑒於此Plugin是作為捐贈和募款平台性質使用，故而攻擊可能會曝露捐贈者的敏感資料，並影響使用該Plugin組織的聲譽，建議使用者/組織應儘速更新至3.14.2版，以避免受到影響。

● 資料來源：

1. [CVE-2024-5932 \(CVSS 10\): Critical RCE Vulnerability Impacts 100k+ WordPress Sites](#)
2. [\\$4,998 Bounty Awarded and 100,000 WordPress Sites Protected Against Unauthenticated Remote Code Exec](#)

2.4 軟硬體漏洞資訊

2.4.1 Avtech攝影機存在高風險安全漏洞

CVE 編號	CVE-2024-7029
影響產品	Avtech 網路攝影機
解決辦法	1.產品已不再維護，建議汰換設備。 2.如仍需使用設備，請留意官方更新資訊，並透過防火牆或相關防護設備限制網際網路 IP 存取攝影機，僅開放 VPN 或特定 IP 來源等連線方式。

- 內容說明：

研究人員發現 Avtech 的網路攝影機(AVM1203)存在命令注入 (Command Injection)漏洞(CVE-2024-7029)，允許未經身分鑑別之遠端攻擊者可利用執行中程式的擁有者身份注入並執行指令，請儘速確認並進行相關防護措施。

陞泰科技發表聲明，指出 AVM1230 為停產近七年的產品，並表示將評估是否釋出修補軟體或提供替代方案。此外，該公司已對目前產品線進行全面檢測，確認目前銷售的機種已經採取相關處理措施或解決方案。

- 影響平台：

AVM1203: 韌體 FullImg-1023-1007-1011-1009(含)以前版本

- 資料來源：

1. <https://nvd.nist.gov/vuln/detail/CVE-2024-7029#VulnChangeHistorySection>
2. <https://www.cisa.gov/news-events/ics-advisories/icsa-24-214-07>
3. <https://www.ithome.com.tw/news/164310>

2.4.2 Microsoft作業系統存在高風險安全漏洞

CVE 編號	CVE-2018-0824
影響產品	Windows
解決辦法	官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下： https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0824

- 內容說明：

近期研究人員發現駭客針對過去發現之重大漏洞進行攻擊，該漏洞為 Microsoft 作業系統存在遠端執行程式碼(Remote Code Execution)漏洞(CVE-2018-0824)，允許未經身分鑑別之遠端攻擊者誘騙使用者下載並執行惡意檔案後，可於使用者端執行任意程式碼。近期發現該漏洞遭駭客利用並攻擊部分台灣研究機構，請儘速確認並進行修補。

- 影響平台：

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems

Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)
Windows Server, version 1803 (Server Core Installation)

● 資料來源：

1. <https://nvd.nist.gov/vuln/detail/CVE-2018-0824>
2. <https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-0824>
3. <https://www.ithome.com.tw/news/164297>

第 3 章、資安研討會及活動

【資安學院-國際證照班】9/19-9/20 ISO/IEC 27001:2022資訊安全管理系統 主導稽核員「轉版」訓練課程（二日）

活動時間	2024-09-19 09:00 ~ 2024-09-20 17:00
活動地點	中華民國資訊軟體協會-大同辦公室D01大會議室（台北市中山區中山北路3段22-1號新設工大樓 5樓 C區）
活動網站	https://www.cisanet.org.tw/Course/Detail/5179

活動概要

中華軟協資安學院

讓您快速升級 火熱報名中

ISO/IEC 27001:2022資訊安全管理系統

主導稽核員 轉版 訓練課程（二日）


ISO/IEC 27001於2022年10月25日正式頒佈新版標準（2022年版），其中的更動如：編輯小幅更動、為符合新的ISO調和結構的更動，以及在安全控制面的要求進行了許多新增及調整。

此課程是針對已取得ISO/IEC 27001:2013年版證書者，提供新舊版本標準的差異介紹，以協助學員能有效的提升對新版標準的瞭解。通過考試者，將由BSI英國標準協會台灣分公司授予轉版證書。

課程資訊

113年9月19日（二）~ 113年9月20日（三）
09:00~17:00，共計二日

中華民國資訊軟體協會-大同辦公室 D01大會議室
（台北市中山區中山北路三段22-1號 新設工大樓5F C區）



報名連結

課程對象

- 資訊安全管理人員、內部稽核人員、電腦稽核人員
- ISO/IEC 27001輔導人員及資訊安全管理系統輔導之顧問
- 持有ISO/IEC 27001:2013主導稽核員證書者

課程費用

- 原價：NT 24,000元/人
- 軟協會員/公家機關：**享最高優惠，請電洽承辦**
- 早鳥價：NT 23,500元/人（113/7/19前完成報名及繳費）
- 四人團報價：NT 23,000元/人
- 費用含稅、教材、餐點及證書

其他資訊

- 講師：BSI台灣分公司專業合格之講師授課(具備ISO/IEC 27001主導稽核員資格)
- 教材：英、中對照教材及試卷
- 證書：BSI原廠授證。課程測驗通過後，將由BSI台灣分公司轉版證書。測驗未通過者，本會則將發「結業證書」乙只。
- 本課程需**全程參與**，**不可請假或缺席**，請假或缺席時數者不予考試及發證，敬請保留完整上課時間。

聯絡資訊：中華軟協資安服務處 林專員
Email: security@cisanet.org.tw Tel: (02)2553-3988 Ext : 816
※主辦單位保留課程、內容及主講者最終變更及調整之權利

【費用】

原價：24,000元/人

早鳥價：23,500元/人(開課前兩個月需完成報名)

公務機關/軟協會員：請致電承辦人

費用含稅、教材、餐點及完課證明

報名截止：2024-09-12

【活動內容 / Event Details】

ISO 27001 隨著數位化改變全球數位格局，如遠端工作、自攜電子設備以及工業 5.0 等商業實務，變得更佳依賴雲端和數位。ISO/IEC 27001 於 2022 年 10 月 25 日正式頒佈新版標準（2022 年版），本次轉課程將協助您快速掌握附錄 A 條款五至八的變化，並能夠幫助組織因應新版 ISO/IEC 27001:2022 標準，以此展現組織資安風險控管績效並強化客戶信任。

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】 02-2553-3988 分機 816 林專員

security@cisnet.org.tw

【資策會】9/27(五)舉辦「零信任資安強化企業防禦韌性」媒合交流會，敬邀產業先進踴躍參加！

活動時間	113年09月27日(五)13：30～16：30(敬備茶點)
活動地點	數位產業署沙資安服務基地5樓共創空間D508室(地址：臺南市歸仁區歸仁13路1段6號)
活動網站	https://ievents.iii.org.tw/EventS.aspx?t=0&id=2581

活動概要

數位發展部數位產業署 廣告

零信任資安

強化企業防禦韌性 媒合交流會

時間：113年09月27日(五)13:30-16:30
地點：沙崙資安服務基地5樓 共創空間D508室
 (地址:台南市歸仁區歸仁十三路一段6號)

隨著企業邁向數位化，地端和雲端的資安部署樣態也越來越多，企業更需要調整自身的資訊安全策略，因應越趨複雜的系統環境、法令規定及新型態的網路攻擊，零信任資安架構幫助企業落實精準的存取權，提升企業無邊界的網路安全，本活動分享零信任架構資安部署的實證經驗，協助企業未來導入零信任架構，強化企業資安韌性。

時間	議程	講師
13:30~14:05	報到與開場	沙崙計畫服務團隊
14:05~14:25	【防禦篇】 零信任資安場域導入經驗	全景軟體股份有限公司 陳建志 規劃顧問
14:25~14:45	【預防篇】 透過零信任架構有效緩解外部攻擊面威脅	奧義智慧科技股份有限公司 鄭宗賢 亞太營運總監
14:45~15:05	【治理篇】 零信任架構提升企業資安治理	瑞思資訊股份有限公司 王英聰 技術長
15:05~15:50	零信任資安解方分組交流	
15:50~16:00	休息與移動到沙崙基地	全體貴賓
16:00~16:30	沙崙基地Testbed導覽	
16:30~	賦歸	

主辦單位 數位發展部 數位產業署
Administration for Digital Industries, moa

執行單位 財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY

【費用】 免費

【活動對象】

正在尋找「零信任資安解決方案」或對零信任架構議題有興趣的企業廠商

【活動人數】

20名(採審核制，以企業廠商為優先；每間廠商以1名為原則，主辦單位視實際報名狀況調整)

【活動方式】

依企業廠商現況與需求進行分組交流，由資安專家提供相關資安防護建議。

【活動內容 / Event Details】

請參考報名網站

【主辦單位】 數位發展部數位產業署

【執行單位】 財團法人資訊工業策進會

【聯絡窗口】 (06)303-2260 分機 535 張小姐 changyunyun@iii.org.tw

【報名截止】 2024-09-23

【資安學院】10/4惡意程式偵測、分析、防護實戰班

活動時間 2024-10-04 09:00 ~ 2024-10-04 16:00

活動地點 中華民國資訊軟體協會-大同辦公室D01大會議室 (台北市中山區中山北路3段22-1號新設工大樓 5樓 C區)

活動網站 <https://www.cisnet.org.tw/Course/Detail/5257>

活動概要

資安學院

惡意程式

偵測、分析、防護實戰班


【費用】

原價：NT 6,900元/人

早鳥價：6,200元/人(課前一個月報名)

軟協會員：NT 5,600元/人

費用含稅、教材、餐點及完課證明

【活動內容 / Event Details】

惡意程式一向為嚴重的資安威脅，從一般的殭屍網路、勒索軟體到精密的 APT 攻擊，惡意程式都扮演重要的攻擊媒介。因此檢測系統中的惡意程式，為相當重要的資安議題。

本課程將介紹各類型的惡意程式及結構，並從 DEMO 操作了解各種惡意程式的行為特徵，如：Backdoor、rootkit、無檔案攻擊等。了解惡意程式的行為後，課程的另一重點為探討在企業組織內部的基礎 IT 架構中，要如何偵測惡意程式，以及主機感染惡意程式後，如何使用分析工具查找惡意程式進而清除。

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisanet.org.tw

【報名截止】 2024-09-27

【資安學院】10/8風險無懼·營運永續—企業IT營運持續管理實戰分析班

活動時間 2024-10-08 09:00 ~ 2024-10-08 16:00

活動地點 中華民國資訊軟體協會-大同辦公室D01大會議室 (台北市中山區中山北路3段22-1號新設工大樓 5樓 C區)

活動網站 <https://www.cisanet.org.tw/Course/Detail/5280>

資安學院

風險無懼·營運永續

—企業IT營運持續管理實戰分析班



活動概要	<p>【費用】</p> <p>原價：NT 6,900元/人 早鳥價：NT 6,200元/人(課前一個月報名) 軟協會員：NT 5,600元/人 費用含稅、教材、餐點及完課證明</p> <p>【活動內容 / Event Details】</p> <p>數位環境的威脅不斷演變，當企業運用科技生產出先進的產品、提供客戶即時便利的服務、追求更高利潤的同時，亦面臨著複雜的資安挑戰，如資訊系統大當機、駭客入侵、勒索病毒等層出不窮，這些威脅可能使得人員作業或資訊設備中斷，造成企業的重大危機。營運持續策略是目前業界應對的有效管理機制，可鑑別出威脅組織的潛在衝擊，提供具有彈性的應對計畫，以維持企業IT的持續運作。</p> <p>本課程先解說營運持續相關法規與標準，接著藉由各項業界實務案例及練習題目，教導學員整合風險管理與營運衝擊分析之方法，提升分析及規劃能力。</p> <p>【主辦單位】 中華民國資訊軟體協會 【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisanet.org.tw 【報名截止】 2024-10-01</p>
<p>【資安學院】10/17駭客入侵防護實務</p>	
活動時間	2024-10-17 09:00 ~ 2024-10-17 16:00
活動地點	中華民國資訊軟體協會-大同辦公室D01大會議室 (台北市中山區中山北路3段22-1號新設工大樓 5樓 C區)
活動網站	https://www.cisanet.org.tw/Course/Detail/5258

**活動概要 【費用】**

原價：NT 6,900元/人

早鳥價：NT 6,200元/人(課前一個月報名)

軟協會員：NT 5,600 元/人

【活動內容 / Event Details】

隨著數位時代的來臨，網路安全議題儼然已成為當代人們不得不關注的問題。網站安全的實用指南，提供全面且易於操作的解決方案。從基礎到進階層面，涵蓋各種網站所需的知識和技巧。本課程內容先介紹基本安全措施，接著透過實務攻擊 DEMO 操作，讓您了解各種入侵思路，如：控制訪問權限、常見網站安全入侵手法等。再進一步強化系統安全，探討安全配置與即時安全監測。以深入淺出的方式，使學員在短時間內掌握駭客入侵防護的重要概念，並能藉此對網路安全有更深刻的理解，且能應用所學。

【主辦單位】 中華民國資訊軟體協會

【聯絡窗口】 02-2553-3988 分機 816 林專員 security@cisanet.org.tw

【報名截止】 2024-09-12

TWCERT/CC 資安活動紀事

活動名稱 113年台灣 CERT/CSIRT 聯盟資安教育訓練(台中場)(113.08.27)

活動時間 113.8.27(二) 14:30~17:00

活動概要



TWCERT/CC於113年08月27日(二)假「集思台中文心會議中心」舉行113年第1場「台灣CERT/CSIRT 聯盟」資安教育訓練，本次訓練特別邀請到法務部調查局游騰葦調查官，講述「資安事件處理的準備與作業方式」與「資安事件通報與應變指引」，並輔以新興資安議題與趨勢，提供全面且實用的資安知識。

游調查官常年從事電腦犯罪調查及網路威脅分析工作，協助公營單位調查網路攻擊及APT駭侵行動。具有EC-Council CEH、CHFI和GIAC GCFA等國際專業證照。

參與者學習如何建立有效的資安事件應變機制，掌握快速準確的通報流程，以及了解最新的資安威脅與防護策略。本課程旨在提升企業的整體資安意識和應變能力，協助建立更安全的數位環境。無論是資安專業人員還是企業決策者，都能從中獲得寶貴的洞見和實務技能。

活動議程	時間	議題	講師
	14:00 – 14:30	報到	
	14:30 – 15:30	講題一：資安事件處理的準備與作業方式	法務部調查局 游騰葦調查官
	15:30 – 15:40	休息/茶敘時間	
	15:40 – 16:40	講題二：資安事件通報與應變指引	法務部調查局 游騰葦調查官
	16:40 – 17:00	意見交流	

第 4 章、TVN 漏洞公告

TWCERT/CC 本月份發布之CVSS 3分數為8.8以上之漏洞資訊如下表：

中興保全 Dr.ID 門禁管理系統 - SQL injection	
TVN / CVE ID	TVN-202408005 / CVE-2024-7731
CVSS	9.8 (Critical) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
影響產品	Dr.ID 門禁管理系統 3.6.3(不含)以前版本
問題描述	中興保全Dr.ID門禁管理系統未妥善驗證特定頁面參數，允許未經身分鑑別之遠端攻擊者注入SQL指令讀取、修改及刪除資料庫內容。
解決方法	更新 Dr.ID 門禁管理系統至 3.6.3(含)以後版本
公開日期	2024-08-13
相關連結	https://www.twcert.org.tw/newepaper/cp-151-8005-c3c94-3.html

中興保全 Dr.ID 考勤管理系統 - Unrestricted File Upload	
TVN / CVE ID	TVN-202408006 / CVE-2024-7732
CVSS	8.8 (High) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
影響產品	Dr.ID 考勤管理系統 3.5.0.0.0.5(不含)以前版本
問題描述	中興保全Dr.ID考勤管理系統未妥善驗證上傳檔案類型，已取得一般權限之遠端攻擊者可上傳網頁後門程式至網頁目錄，並利用該後門程式於遠端伺服器執行任意程式碼。

解決方法	更新 Dr.ID 考勤管理系統至 3.5.0.0.0.5(含)以後版本
公開日期	2024-08-13
相關連結	https://www.twcert.org.tw/newepaper/cp-151-8007-803d6-3.html

編輯：TWCERT/CC 團隊

發行單位：台灣電腦網路危機處理暨協調中心

(Taiwan Computer Emergency Response Team / Coordination Center)

出刊日期：2024年 8月 30 日

電子郵件：CERT_Service@cert.org.tw

官網：<https://twcert.org.tw/>

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

Instagram：<https://www.instagram.com/twcertcc/>