區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 資通安全管理法
- 資安案例分享
  - 釣魚郵件攻擊案例
  - SSL VPN重大漏洞

大 綱

- 資通安全管理法
- 資安案例分享
  - 釣魚郵件攻擊案例
  - SSL VPN重大漏洞

B 級之公務機關應辦事項

管理面

辦理項目	辦理項目細項	辦理內容
資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；須以專職人員配置之。
內部資通安全稽核		每年辦理一次。
業務持續運作演練		全部核心資通系統每二年辦理一次。
資安治理成熟度評估		每年辦理一次。
限制使用危害國家資通安全產品		一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務網路環境介接。

B 級之公務機關應辦事項

技術面

技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。
	政府組態基準		初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	

B 級之公務機關應辦事項

認知與訓練

認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證照之有效性。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證書之有效性。

C 級之公務機關應辦事項

管理面

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	限制使用危害國家資通安全產品		一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務網路環境介接。

C 級之公務機關應辦事項

技術面

技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	

15

		目錄伺服器設定及防火牆連線設定檢視	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

C 級之公務機關應辦事項

認知與訓練

認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	資通安全專職人員總計應持有一張以上，並持續維持證照之有效性。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有一張以上，並持續維持證書之有效性。

D 級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	限制使用危害國家資通安全產品		一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務（業務）網路環境介接。
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。

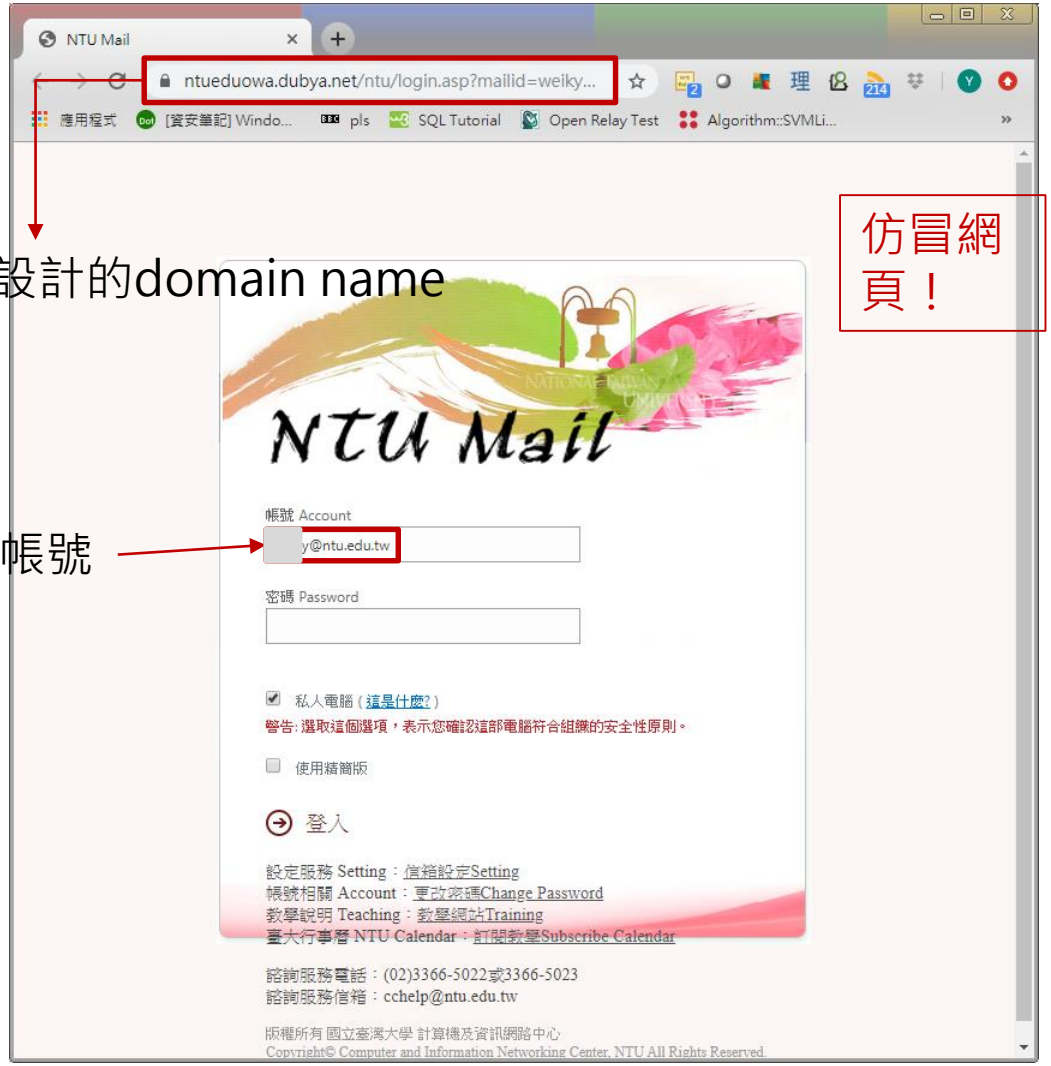
大 綱

- 資通安全管理法
- 資安案例分享
  - 釣魚郵件攻擊案例
  - SSL VPN重大漏洞

假冒系統管理員寄信騙取帳密

- 針對NTU OWA設計的domain name
- 具安全憑證

已填入欲騙取之帳號



大 綱

- 資通安全管理法
- 資安案例分享
  - 釣魚郵件攻擊案例
  - SSL VPN重大漏洞

Palo Alto SSL VPN 漏洞

簡介

- 戴夫寇爾研究團隊(後續簡稱研究團隊)在進行紅隊(Red Team)演練的過程中，發現目標使用的 Palo Alto GlobalProtect 存在 format string 弱點，透過此弱點可控制該 SSL VPN 伺服器，並藉此進入內網
- GlobalProtect是Palo Alto的SSL VPN產品
- 該研究團隊回報原廠後，得知這是個已知弱點並且已經 silent-fix
- 此漏洞編號為CVE-2019-1579* ； Palo Alto發布漏洞編號為PAN-SA-2019-0020

備註：

1. 通報到Palo Alto時，那時候Palo Alto回覆是沒有CVE編號，是Palo Alto後來更新資訊並補上CVE編號

圖片來源：
https://www.paloaltonetworks.tw/resources/datasheets/globalprotect-datasheet

影響範圍

- 存在漏洞的版本如下，建議用戶儘速更新至最新版以避免遭受攻擊：
  - ✓Palo Alto GlobalProtect SSL VPN 7.1.x < 7.1.19
  - ✓Palo Alto GlobalProtect SSL VPN 8.0.x < 8.0.12
  - ✓Palo Alto GlobalProtect SSL VPN 8.1.x < 8.1.3
- 9.x 和 7.0.x 並沒有存在此漏洞

漏洞分析

- “**sslmgr**”是被用來處理Server端和Client端之間SSL handshake的服務
- 在研究跟“**sslmgr**”有關的資料中，研究團隊發現“**scep-profile-name**”的字串會用“**snprintf**”的格式存入buffer中
- 他們就針對這個特性發動攻擊，例如塞入大量不重要資料造成這個服務crash

建議措施

- 升級Palo Alto GlobalProtect SSL VPN到
  a. 7.1.18及之前的版本 升級至 7.1.19 或以後的版本
  b. 8.0.11及之前的版本 升級至 8.0.12 或以後的版本
  c. 8.1.2 及之前的版本 升級至 8.1.3 或以後的版本

Fortigate SSL VPN 漏洞

簡介

- Fortigate SSL VPN是Fortinet旗下SSL VPN產品
- 這些CVE漏洞已先通報原廠，等廠商修好漏洞後才公開
- 研究團隊在black hat USA 2019公布了五個Fortigate SSL VPN與七個Pulse Secure SSL VPN的漏洞

圖片來源：https://www.fortinet.com/tw

CVE漏洞一覽

- 研究團隊發現以下這五個漏洞：
  - CVE-2018-13379：Pre-auth arbitrary file reading
  - CVE-2018-13380：Pre-auth XSS
  - CVE-2018-13381：Pre-auth heap overflow
  - CVE-2018-13382：Modify anyuser’s password with a magic key
  - CVE-2018-13383：Post-auth heap overflow
- 被紅色標記是在Github上有相關PoC程式

影響範圍

CVE-2018-13379
- FortiOS 5.4 - 5.4.6 to 5.4.12
- FortiOS 5.6 - 5.6.3 to 5.6.7
- FortiOS 6.0 - 6.0.0 to 6.0.4

CVE-2018-13380
- FortiOS 5.4 and below
- FortiOS 5.6 - 5.6.0 to 5.6.7
- FortiOS 6.0 - 6.0.0 to 6.0.4

CVE-2018-13381
- FortiOS 5.4 and below
- FortiOS 5.6 - 5.6.0 to 5.6.7
- FortiOS 6.0 - 6.0.0 to 6.0.4

CVE-2018-13382
- FortiOS 5.4 - 5.4.1 to 5.4.10
- FortiOS 5.6 - 5.6.0 to 5.6.8
- FortiOS 6.0 - 6.0.0 to 6.0.4

CVE-2018-13383
- FortiOS 5.6.10 and below
- FortiOS 6.0 - 6.0.0 to 6.0.4

建議措施

- 整理出官方建議升級版本資訊如下：
  - FortiOS 5.4 – 5.4.13 或之後更新的版本
  - FortiOS 5.6 – 5.6.11 或之後更新的版本
  - FortiOS 6.0 – 6.0.5　或之後更新的版本
- 升級至 FortiOS 6.2.0

Pulse Secure SSL VPN 漏洞

簡介

- 研究團隊花費許多時間找出Pulse Secure SSL VPN的漏洞
- Pulse Secure是用Perl開發，並使用C++擴展功能，這讓挖掘漏洞的難度提昇不少
- 今年3/8找到第一個漏洞，並且3/22通報Pulse Secure
- Pulse Secure 接獲漏洞通知後，在一個月內 (4/24)發布了修補更新檔

圖片來源：https://www.pulsesecure.net/

CVE漏洞一覽

- 研究團隊發現以下這7個漏洞：
  - CVE-2019-11507：Cross-site scripting
  - CVE-2019-11508：Post-auth NFS arbitrary file writing
  - CVE-2019-11510：Pre-auth arbitrary file reading
  - CVE-2019-11538：Post-auth NFS arbitrary file reading
  - CVE-2019-11539：Post-auth command injection
  - CVE-2019-11540：XSSI session hijacking
  - CVE-2019-11542：Post-auth stack buffer overflow
- 被紅色標記是在Github上有相關PoC程式

影響範圍

- Pulse Connect Secure 9.0R1 – 9.0R3.3
- Pulse Connect Secure 8.3R1 – 8.3R7
- Pulse Connect Secure 8.2R1 – 8.2R12
- Pulse Connect Secure 8.1R1 – 8.1R15
- Pulse Policy Secure 9.0R1 – 9.0R3.3
- Pulse Policy Secure 5.4R1 – 5.4R7
- Pulse Policy Secure 5.3R1 – 5.3R12
- Pulse Policy Secure 5.2R1 – 5.2R12
- Pulse Policy Secure 5.1R1 – 5.1R15

建議措施

- 請升級至下列版本：
  - Pulse Connect Secure 9.1R1 and above
  - Pulse Connect Secure 9.0R4 & 9.0R3.4
  - Pulse Connect Secure 8.3R7.1
  - Pulse Connect Secure 8.2R12.1
  - Pulse Connect Secure 8.1R15.1
  - Pulse Policy Secure 9.1R1 and above
  - Pulse Policy Secure 9.0R4 & 9.0R3.4
  - Pulse Policy Secure 5.4R7.1
  - Pulse Policy Secure 5.3R12.1
  - Pulse Policy Secure 5.2R12.1
  - Pulse Policy Secure 5.1R15.1

備註：
詳細資訊可以參考官方網站：
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

Q & A