

# 桃園區網中心

## 第62次區網會議

國立中央大學 電算中心

107年10月25



# 桃園區網中心概況報告

資訊安全攻擊行為

資訊安全攻擊事件、防範措施

網管通訊錄更新



# 資訊安全攻擊行為

## 病毒式釣魚信件攻擊

電子郵件威脅存在多年，儘管防護功能與資安意識也不斷演進，但釣魚郵件也在進化，而現在愈來愈多網路攻擊以此做為開端，令人防不勝防。

普遍這些攻擊的一開始，多半是透過電子郵件、即時通訊軟體與社群網站作為管道，可能引導用戶至假冒的釣魚網站，騙取用戶個人資訊及密碼，進而成為網路詐騙、勒索、滲透等一連串網路攻擊的開端。

## CLDAP 反射式放大攻擊

相較於一般反射型攻擊手法可能需入侵上百萬台主機，但**CLDAP**反射式放大攻擊，具有破壞性且有效的**DDoS**攻擊。僅需少數主機就能產生大量的攻擊頻寬，使**DDoS**攻擊的規模越來越大。

攻擊者的頻寬有限，但透過向伺服器傳送小型的訊息，伺服器會回應給受害者大量的回應。



## 資訊安全攻擊行為(續)

### 漏洞預警

雖然企業修補漏洞的速度已經有所改進，但仍趕不上漏洞攻擊的加速度。因為系統的漏洞、程序撰寫的錯誤及管理人員的疏忽，使得駭客有機可乘。

要防禦這類的攻擊，使用弱點掃描產品是基本配備，對於各校有提供**EVS**網站，做弱點掃描服務，定時對系統、網站進行弱點掃描，即時掌握系統及網站的安全。





# 病毒式釣魚信件攻擊事件

釣魚信件以「回覆(Reply)」型態發動攻擊，分析說明如下：

1. 寄件者為曾經通過信的人
2. 郵件主旨為之前通信的主旨
3. 開啟信件時出現錯誤訊息「**Unable to show this message**」，誘使收件者點擊信件中的訊息按鈕「**Click here to view message**」。接著轉導至仿造的學校郵件網頁，讓不知情的收件者輸入自己的帳號及密碼，導致郵件帳密被盜取，形同中毒接續下一波的釣魚信攻擊。

影響平台： 個人電子郵件帳密被盜取

[建議措施:]

1. 勿理會該信件，通知學校郵件管理者或資安人員。
2. 如果已經輸入了帳號及密碼，請盡快至學校修改密碼之網頁，修改密碼。
3. 定期更新主機防毒軟體及全機掃描。



# CLDAP反射性放大攻擊事件

## [內容說明]

學術網路中發現有不少**DDOS攻擊**，使用**CLDAP反射式放大攻擊 ( UDP PORT 389)**。其中，有不少學校也成為攻擊幫兇，因其**LDAP服務的 UDP PORT 389 (CLDAP)**暴露於網路上，進而遭人利用。

其攻擊係**透過查詢AD的ROOTDSE時**，預設情況下**不需要權限**，並**透過UDP類型之PROTOCOL：CLDAP (PORT 389)**即可存取的狀況下，**偽造來源查詢封包**，以攻擊受害者電腦。

### • [影響平台:]

使用**LDAP服務之主機**。

### • [建議措施:]

1. 服務主機可**架設防火牆進行ACL的控管**。
2. 於設定檔中**關閉ANONYMOUS ACCESS**。
3. **CLDAP PROTOCOL (UDP PORT 389)**應避免暴露於**INTERNET**上。



# ANA-漏洞預警

## • [內容說明]:

• **JUNIPER JUNOS OS**是**JUNIPER NETWORKS**公司一套以**FREEBSD**為基礎所發展，專用於該公司網路設備的作業系統。

近而發現，**JUNOS OS**之**NTP**套件存在多個安全漏洞，肇因於**SSHD**預設將「**PERMITEMPTYPASSWORDS**」選項設定為「**YES**」，又以**CVE-2018-7183**最為嚴重，當攻擊者針對使用**JUNOS OS**的網路設備進行**NTP**功能查詢時，藉由發送特製的惡意封包可使其**DECODEARR**函數出現緩衝區溢位情況，導致攻擊者可遠端執行任意程式碼。

## [影響平台]:

**JUNIPER NFX**系列之**JUNOS OS 18.1**至**18.1R4**以前版本 包含：

• **J系列** • **M系列** • **T系列** • **MX系列** • **EX系列** • **SRX系列** • **QFX系列** • **NFX系列** • **PTX系列**

## [建議措施]:

目前**JUNIPER**官方已針對弱點釋出修復版本，將**JUNOS OS**升級至以下版本：

- **12.1X46-D77** • **12.3X48-D70** • **12.3X54-D34** • **12.3R12-S10** • **12.3R13** • **14.1X53-D47**
- **15.1X49-D140** • **15.1X53-D490** • **15.1X53-D471** • **15.1X53-D234** • **15.1X53-D67** • **15.1X53-D59**
- **15.1R4-S9** • **15.1R7-S1** • **15.1R8** • **16.1R4-S9** • **16.1R6-S4** • **16.1R7** • **16.2R1-S7**
- **16.2R2-S6** • **16.2R3** • **17.1R1-S7** • **17.1R2-S7** • **17.1R3** • **17.2R1-S6** • **17.2R2-S4**
- **17.2R3** • **17.3R1-S5** • **17.3R2-S2** • **17.3R3** • **17.4R1-S4** • **17.4R2** • **18.1R2** • **18.2X75-D5**
- **18.2R1**



# 宣導事項

桃園區網聯絡人：陳奕翰

Email：center79@cc.ncu.edu.tw

電話：03 -4227151#57514

## 網管通訊錄更新

若單位名稱、網管人員及聯絡方式有變動，請與區網聯絡更新。



## 教育訓練|講座|會議

原則上都安排在星期四



## 校園資安推廣

推廣對象：教職員及學生均可

徵求連線單位講師支援(具有資安相關證照及相關研究)