張貼日期：2018/09/04

[資安漏洞預警通知] CLDAP 反射式放大攻擊，請各單位注意防範，並避免遭利用

主旨：[資安漏洞預警通知] CLDAP 反射式放大攻擊，請各單位注意防範，並避免遭利用

- 內容說明：
  - 近期，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。
- 影響平臺：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。
- 參考資料:
  1. https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf
  2. https://www.us-cert.gov/ncas/alerts/TA14-017A

計算機與通訊中心
網路系統組 敬啟