

NTP校時服務攻擊(NTP-reflection attacks)

計通中心近日由網路系統記錄發現校園網路上的UDP 123 port 流量輸出異常，經查為校園內啟用 NTP 服務的網路設備，遭利用於攻擊他人網路頻寬。

NTP 攻擊之原理與 DNS 放大攻擊相同。NTP 協定使用 UDP 123 Port 傳輸，設定不當的 NTP 校時伺服器，即可被用來攻擊他人網路頻寬。其中 NTP 的 monlist 指令，可透過偽造來源 IP 反射至被攻擊端外，亦具有 query/response 倍數差異的放大效果。

NIST - NVD(National Vulnerability Database) 於今年 1 月 2 日公布此弱點 CVE-2013-5211 (詳見參考資料1)。Cisco 亦於 1 月 15 日發布 Cisco IOS 弱點警訊 (Cisco NTP Distributed Reflective Denial of Service Vulnerability) 並指出 IOS 內 NTP 套件之 MODE_PRIVATE (Mode 7) 指令可能被利用於 NTP 攻擊 (詳見參考資料2)。

由於此弱點存在於 NTP 版本 4.2.7p26 以下，建議各單位將 NTP 升級至少至版本 4.2.7p26 (目前已釋出版本 4.2.7p424) 以防此事件發生。另外可透過 NTP Scanning Project (詳見參考資料3) 進行檢測，亦可參考 Team Cymru 提供之網路設備 NTP 服務及防火牆之設定模板 (詳見參考資料4)，以避免類似攻擊發生。

參考資料

1. <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5211>
2. <http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5211>
3. <http://openntpproject.org>
4. <http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html>

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/security:attack:ntp_attack



Last update: **2014/03/04 15:18**