張貼日期：2017/09/21

[資安漏洞預警通知] D-Link DIR-850L AC1200雙頻Gigabit無線路由器存在多個漏洞，允許攻擊者遠端執行任意程式碼或造成阻斷服務

主旨：D-Link DIR-850L AC1200雙頻Gigabit無線路由器存在多個漏洞，允許攻擊者遠端執行任意程式碼或造成阻斷服務

說明：

1. 友訊科技(D-Link)為臺灣網路設備的製造商，旗下產品包含路由器、無線網卡、視訊鏡頭及儲存硬碟等。
2. 南韓研究人員Pierre Kim在今年9月公開揭露D-Link所生產之DIR-850L AC1200雙頻Gigabit無線路由器的韌體存在多個安全漏洞(CVE-2017-14413~CVE-2017-14430)，可能導致下列多項資安風險：
    1. 允許攻擊者可遠端執行跨網站腳本攻擊。
    2. 因未使用加密傳輸協定，導致攻擊者可透過中間人攻擊方式獲取帳號密碼等資訊。
    3. 攻擊者可遠端執行任意程式碼或造成阻斷服務。
3. 影響平臺：
   D-Link 850L韌體版本小於1.14.B07版本
   D-Link 850L韌體版本小於2.07.B05版本
4. 建議措施：
    1. 請檢查所使用之韌體是否為受影響之版本，檢查方式
        1. 登入DIR-850L管理介面，
        2. 點選「工具」，
        3. 點選「韌體」，即可看到目前所使用之韌體版本與韌體日期資訊。
    2. 目前D-Link官方尚未針對此弱點釋出修復的韌體版本，若使用韌體為受影響版本，請持續關注D-Link官方網頁釋出的韌體更新版本。
5. 參考資料:
    1. http://thehackernews.com/2017/09/d-link-router-hacking.html
    2. https://pierrekim.github.io/blog/2017-09-08-dlink-850l-mydlink-cloud-0days-vulnerabilities.html
    3. http://support.dlink.com/ProductInfo.aspx?m=DIR-850L

計算機與通訊中心
網路系統組 敬啟

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/mailing:announcement:20170921_01

Last update: **2017/09/21 10:10**