# 行政院國家資通安全會報技術服務中心

# 漏洞/資安訊息警訊

| | | | |
|---|---|---|---|
| 發布編號 | NCCST-ANA-2017-0097 | 發布時間 | Tue Sep 19 10:01:01 CST 2017 |
| 事件類型 | 漏洞預警 | 發現時間 | Mon Sep 18 00:00:00 CST 2017 |
| 警訊名稱 | 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 | | |
| 內容說明 | 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。<br><br>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：<br><br>1.允許攻擊者可遠端執行跨網站腳本攻擊。<br><br>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。<br><br>3.攻擊者可遠端執行任意程式碼或造成阻斷服務。 | | |
| 影響平台 | D-Link 850L 韌體版本小於 1.14.B07 版本<br><br>D-Link 850L 韌體版本小於 2.07.B05 版本 | | |
| 影響等級 | 高 | | |
| 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。<br><br>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。 | | |
| 參考資料 | 1.http://thehackernews.com/2017/09/d-link-router-hacking.html<br><br>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 |

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw