張貼日期：2020/06/18

【資安漏洞預警】D-Link DIR-865L路由器存在六個資安漏洞，請儘速確認並進行更新！

主旨：【資安漏洞預警】D-Link DIR-865L路由器存在六個資安漏洞，請儘速確認並進行更新！

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-ANA-202006-0017】
  - D-Link DIR-865L路由器存有六個資安漏洞，分別為：
    1. Improper Neutralization of Special Elements Used in a Command (Command Injection): 攻擊者可以利用URL參數注入Command進行攻擊。
    2. Cross-Site Request Forgery (CSRF): 攻擊者進行CSRF攻擊繞過身分驗證來查看、刪除任意檔案，或是上傳惡意檔案等。
    3. Inadequate Encryption Strength: 使用弱加密的方式傳送訊息，可以透過暴力攻擊來取得用戶的資訊。
    4. Predictable seed in pseudo-random number generator: 使用者登入時的信息(cookie, challenge, public key)】是由一個function所生成random seed進行加密，但該function中將登錄時間設為random seed】使攻擊者可以輕易破解。
    5. Cleartext storage of sensitive information: 在PHP頁面中使用明文儲存管理者密碼。
    6. Cleartext transmission of sensitive information: 使用明文的方式傳輸，攻擊者可以攔截封包來竊取使用者的資訊。
  - CVE編號】CVE-2020-13782】CVE-2020-13783】CVE-2020-13784】CVE-2020-13785】CVE-2020-13786】CVE-2020-13787
  - CVSS3.1】
    - CVE-2020-13782(9.8】CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
    - CVE-2020-13783(7.5】CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
    - CVE-2020-13784(7.5】CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
    - CVE-2020-13785(7.5】CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
    - CVE-2020-13786(8.8】CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
    - CVE-2020-13787(7.5】CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
- 影響平台：
  D-Link DIR-865L路由器
- 建議措施：
  檢視相關設備，並依照原廠建議進行處置。
- 參考資料：
  https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10174

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:20200618_02

Last update: **2020/06/18 14:11**