張貼日期：2023/05/04

【資安漏洞預警】仲琦科技 Hitron CODA-5310 存在多高風險漏洞

- 主旨說明：仲琦科技 Hitron CODA-5310 存在多高風險漏洞

- 內容說明：
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-ANA-202305-0001
  - 仲琦科技 Hitron CODA-5310 存在多個漏洞(CVE-2023-30604、CVE-2023-30603、CVE-2023-30602、CVE-2022-47617、CVE-2022-47616)、其中CVE-2023-30604 與CVE-2023-30603 CVSS 3.1高達 9.8分，遠端攻擊者不須權限，即可查看一般使用者及管理者的帳號密碼、對系統進行任意操作或中斷服務。
  - 以下為各漏洞說明:
    - CVE-2023-30604:仲琦科技CODA-5310 未對所有系統設定網頁進行權限驗證，導致遠端攻擊者不須身分驗證就可以存取特定的系統設定介面，並對系統進行任意操作或中斷服務。
    - CVE-2023-30603仲琦科技CODA-5310 的telnet 功能使用預設帳號和密碼，且未提醒使用者修改，導致遠端攻擊者不須權限即可利用該帳號密碼取得管理者權限，進行查看與修改，造成系統服務中斷。
    - CVE-2023-30602仲琦科技CODA-5310的telnet功能使用明文傳輸敏感資料，導致遠端攻擊者不須權限，即可查看一般使用者及管理者的帳號密碼。
    - CVE-2022-47617仲琦科技CODA-5310將加解密金鑰以hard-coded的方式寫在程式碼中，導致擁有管理者權限的遠端攻擊者可以使用該金鑰，解密系統檔案後進行查看與修改，造成系統服務中斷。
    - CVE-2022-47616仲琦科技CODA-5310的測試連線功能未對特定參數進行過濾，導致擁有管理者權限的遠端攻擊者可以透過管理介面，進行Command Injection攻擊，即可執行系統任意指令，進行任意系統操作或中斷服務。
- 影響平台：
  - Hitron CODA-5310 v7.2.4.7.1b3
- 建議措施：
  - 仲琦科技已提供解決問題版本給網路營運商並告知升級，如有任何問題請聯繫網路提供業者。
- 參考資料：
  1. https://www.twcert.org.tw/tw/cp-132-7082-373d5-1.html
  2. https://www.twcert.org.tw/tw/cp-132-7084-74e83-1.html
  3. https://www.twcert.org.tw/tw/cp-132-7085-13321-1.html
  4. https://www.twcert.org.tw/tw/cp-132-7086-35622-1.html
  5. https://www.twcert.org.tw/tw/cp-132-7083-94e13-1.html

—- 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:20230504_02

Last update: **2023/05/05 09:43**