Le0nC Blog

有什麼 說什麼

網誌存檔

10月 2021 (1)

8月 2021 (1)

4月 2021 (1)

2021年4月22日 星期四

[CVE-2021-26797] An access control vulnerability in Hame SD1 Wi-Fi

Title: An access control vulnerability in Hame SD1 Wi-Fi

Vendor of the product(s)：HAME

Product：Hame SD1 Wi-Fi Product

Version：V. 20140224154640

Vulnerability information：

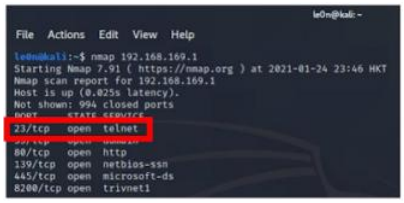
A broken access control vulnerability (weak password) in HAME SD1 wifi, Firmware version <=v.20140224154640 allows an attacker to easily perform brute-force attack to access telnet service and obtain system administrator privilege.

According to OWASP IoT TOP 10 2018:

No1. Weak, Guessable, or Hardcoded Passwords Use of easily brute-forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

PoC:

Using NMAP to scan target device, and found telnet service was open (port 23).



Using Hydra to perform a brute-force attack to get login account and password. (weak password)

Logging in via telnet with the above account and password to obtain system administrator privileges.

at 4月 22, 2021

沒有留言:

張貼留言

如要留言，請點按下方的按鈕使用 Google 帳戶登入。

較新的文章 首頁

訂閱： 張貼留言 (Atom)

搜尋此網誌

搜尋

關於我自己

Le0nC

工照做、盡量做、不包好、錢照收

檢視我的完整簡介