張貼日期：2023/11/03

【漏洞預警□F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2023-46747)□請儘速確認並進行更新。

- 主旨說明□F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2023-46747)□允許攻擊者繞過身分鑑別程序，進而遠端執行任意程式碼，請儘速確認並進行更新。
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202311-00000018□
  - 研究人員發現F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2023-46747)□允許攻擊者於未經身分鑑別之情況下，透過管理連接埠或Self IP位址，存取BIG-IP系統並遠端執行任意程式碼。
- 影響平台:無
- 建議措施:
  1. 目前F5官方已針對此漏洞釋出修復版本，請各機關可聯絡設備維護廠商或參考官方說明(https://my.f5.com/manage/s/article/K000137353)之□Security Advisory Status□一節進行更新：
     1. 連線至網址：https://my.f5.com/manage/s/downloads□
     2. 依所使用之模組與版本下載更新檔。
     3. 使用設備之管理頁面功能更新至最新版本。
  2. 若目前所使用之版本因已停止支援而未釋出修補程式，建議升級至仍有支援且已推出修補程式之版本。
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2023-46747
  2. https://www.ithome.com.tw/news/159530
  3. https://my.f5.com/manage/s/article/K000137368
  4. https://my.f5.com/manage/s/article/K000137353

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:20231103_01

Last update: **2023/11/03 15:38**