張貼日期：2022/05/11

【資安漏洞預警□F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2022-1388)□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-2022-1388)□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-ANA-202205-0423
  - 研究人員發現F5 Networks之BIG-IP產品存在高風險安全漏洞(CVE-2022-1388)□允許攻擊者繞過iControl REST元件之身分鑑別程序，進而存取BIG-IP系統，並遠端執行任意程式碼。
- 影響平台:
  受影響之BIG-IP(All modules)版本如下：
  - 16.1.0-16.1.2
  - 15.1.0-15.1.5
  - 14.1.0-14.1.4
  - 13.1.0-13.1.4
  - 12.1.0-12.1.6
  - 11.6.1-11.6.5
- 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://support.f5.com/csp/article/K23605346)之□Security Advisory Status□一節進行更新：
     1. 連線至網址：https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20LTM □
     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。3.若無法更新至最新版本，請參考F5官方網頁(https://support.f5.com/csp/article/K23605346)之□Mitigation□一節，採取緩解措施：
     1. 禁止透過設備之self IP位址存取iControl REST介面。
     2. 僅允許受信任之使用者與設備可透過BIG-IP設備管理頁面存取iControl REST介面。
     3. 調整BIG-IP設備之httpd設定檔。
- 參考資料:
  1. https://www.ithome.com.tw/news/150831
  2. https://nvd.nist.gov/vuln/detail/CVE-2022-1388
  3. https://support.f5.com/csp/article/K23605346
  4. https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20LTM

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:20220511_01

Last update: **2022/05/11 10:31**