

張貼日期：2020/07/07

【資安漏洞預警】F5 BIG-IP產品存在安全漏洞(CVE-2020-5902與CVE-2020-5903)允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

主旨：【資安漏洞預警】F5 BIG-IP產品存在安全漏洞(CVE-2020-5902與CVE-2020-5903)允許攻擊者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 行政院國家資通安全會報技術服務中心 資安訊息警訊 (NISAC-ANA-202007-0266)
 - F5 BIG-IP產品之流量管理用戶介面(Traffic Management User Interface簡稱TMUI)存在安全漏洞(CVE-2020-5902與CVE-2020-5903)遠端攻擊者可對目標設備發送特製請求，利用此漏洞進而遠端執行系統指令、寫入與刪除檔案、關閉服務及執行任意Java程式碼。
- 影響平台：
 - BIG-IP 15.x: 15.1.0/15.0.0
 - BIG-IP 14.x: 14.1.0 ~ 14.1.2
 - BIG-IP 13.x: 13.1.0 ~ 13.1.3
 - BIG-IP 12.x: 12.1.0 ~ 12.1.5
 - BIG-IP 11.x: 11.6.1 ~ 11.6.5
- 建議措施：
 1. 目前F5官方已針對此弱點釋出更新程式，請各機關聯絡設備維護廠商登入設備管理介面進行版本確認，並更新至下列對應版本：
 - BIG-IP 15.x: 15.1.0.4
 - BIG-IP 14.x: 14.1.2.6
 - BIG-IP 13.x: 13.1.3.4
 - BIG-IP 12.x: 12.1.5.2
 - BIG-IP 11.x: 11.6.5.2
 2. 若無法立即更新，可參考官網公告採取緩解措施：<https://support.f5.com/csp/article/K52145254>
- 參考資料：
 1. <https://support.f5.com/csp/article/K52145254>
 2. <https://www.ithome.com.tw/news/138576>
 3. <https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller>

計算機與通訊中心
網路系統組 敬啟

From:

<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

http://net.nthu.edu.tw/netsys/mailling:announcement:20200707_01

Last update: **2020/07/07 10:15**

