行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2020-0069	發布時間	Mon Jul 06 14:26:20 CST 2020
事件類型	漏洞預警	發現時間	Sun Jul 05 00:00:00 CST 2020
警訊名稱	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	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	受影響 BIG-IP 版本如下: 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		
影響等級	高		
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/

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw