

張貼日期：2021/03/12

【資安漏洞預警】F5 Networks之BIG-IP產品與BIG-IQ產品存在安全漏洞(漏洞編號為CVE-2021-22986至CVE-2021-22992等共7個漏洞), 請儘速確認並進行更新!

- 主旨說明：【資安漏洞預警】F5 Networks之BIG-IP產品與BIG-IQ產品存在安全漏洞(漏洞編號為CVE-2021-22986至CVE-2021-22992等共7個漏洞), 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-202103-0540
 - 研究人員發現F5 Networks之BIG-IP產品與BIG-IQ產品存在安全漏洞(CVE-2021-22986~CVE-2021-22992等共7個漏洞), 遠端攻擊者可利用這些弱點, 藉由發送特製封包或存取未公開頁面, 進而執行任意程式碼並獲得設備主控權。
- 影響平台:
受影響之BIG-IP產品與BIG-IQ產品版本如下：
 1. CVE-2021-22986
 - BIG-IP (All modules)
 - 16.0.0-16.0.1
 - 15.1.0-15.1.2
 - 14.1.0-14.1.3.1
 - 13.1.0-13.1.3.5
 - 12.1.0-12.1.5.2
 - BIG-IQ
 - 7.1.0-7.1.0.2
 - 7.0.0-7.0.0.1
 - 6.0.0-6.1.0
 2. CVE-2021-22987與CVE-2021-22988
 - BIG-IP (All modules)
 - 16.0.0-16.0.1
 - 15.1.0-15.1.2
 - 14.1.0-14.1.3.1
 - 13.1.0-13.1.3.5
 - 12.1.0-12.1.5.2
 - 11.6.1-11.6.5.2
 3. CVE-2021-22989、CVE-2021-22990及CVE-2021-22992
 - BIG-IP Advanced WAF/ASM
 - 16.0.0-16.0.1
 - 15.1.0-15.1.2
 - 14.1.0-14.1.3.1
 - 13.1.0-13.1.3.5
 - 12.1.0-12.1.5.2
 - 11.6.1-11.6.5.2

4. CVE-2021-22991

- BIG-IP (All Modules)
- 16.0.0-16.0.1
- 15.1.0-15.1.2
- 14.1.0-14.1.3.1
- 13.1.0-13.1.3.5
- 12.1.0-12.1.5.2

- 建議措施:

目前F5 Networks官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商或參考以下網址進行更新：

1. <https://support.f5.com/csp/article/K02566623>
2. <https://support.f5.com/csp/article/K03009991>
3. <https://support.f5.com/csp/article/K18132488>
4. <https://support.f5.com/csp/article/K70031188>
5. <https://support.f5.com/csp/article/K56142644>
6. <https://support.f5.com/csp/article/K45056101>
7. <https://support.f5.com/csp/article/K56715231>
8. <https://support.f5.com/csp/article/K52510511>

- 參考資料:

1. <https://support.f5.com/csp/article/K02566623>
2. <https://us-cert.cisa.gov/ncas/current-activity/2021/03/10/f5-security-advisory-rce-vulnerabilities-big-ip-big-iq>

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/mailling:announcement:20210312_01

Last update: **2021/03/12 14:50**

