|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | 遠端命令執行(RCE) | Site | 國立中山大學 |
| URL(s) | http://140.117.103.218:8080/cgi-bin/ | | |
| Risk | 嚴重 | | |
| Details | 國立中山大學QNAP NAS存在CVE-2019-7192、CVE-2019-7193、CVE-2019-7194及CVE-2019-7195等漏洞，Cvss v3風險評分皆為重大(9.8分)，上述漏洞係QNAP NAS設備使用之Photo Station應用程式，存在任意檔案讀取與程式碼注入等安全漏洞，駭客可對目標設備發送出特製的封包請求，進而達到執行任意程式碼。 | | |
| Remedy | QNAP NAS係用來儲存重要資料的設備，為避免遭駭客竊取相關機敏資訊，建議該單位的資訊人員，立即修補漏洞並將設備更新至最新版本。 | | |
| Proofs |  | | |
| Verification |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | 本地檔案引入(LFI) | Site | 剛谷科技股份有限公司 |
| URL(s) | https://210.61.78.120/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd | | |
| Risk | 嚴重 | | |
| Details | 剛谷科技F5 Networks BIG-IP產品存有CVE-2020-5902漏洞，Cvss v3風險評分為重大(10分)，可能讓不具授權的遠端攻擊者執行指令，並取得系統完整控制權，包括攔截流經該設備的應用流量。 | | |
| Remedy | 為避免遭駭客竊取相關機敏資訊，建議該單位的資訊人員，立即修補漏洞並將設備更新至最新版本。 | | |
| Proofs |  | | |
| Verification |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | 資訊洩漏 (Info Leakage) | Site | 台北市政府 |
| URL(s) | http://www.voip.taipei.gov.tw/getwebcallhtml2.asp | | |
| Risk | 低 | | |
| Details | 該網站程式碼洩露(i 後端asp程式碼)，如上述網址及下圖所示。 | | |
| Remedy | 建議針對後端程式碼進行管理調整，非必要對外公開。 | | |
| Proofs |  | | |
| Verification |  | | |