# 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-2019-0071 | 發布時間 | Thu Jun 06 10:34:31 CST 2019 |
| 事件類型 | 漏洞預警 | 發現時間 | Fri May 31 00:00:00 CST 2019 |
| 警訊名稱 | 京晨科技(NUUO Inc.)網路監控錄影系統(Network Video Recorder, NVR)存在安全漏洞(CVE-2019-9653)，允許攻擊者遠端執行系統指令，請儘速確認並進行韌體版本升級 | | |
| 內容說明 | NUUO NVR 是一個以嵌入式 Linux 為基礎的網路監控錄影系統，可同時管理多個網路攝影機，並將影像回傳至儲存媒體或設備。本中心研究團隊發現多款 NUUO NVR 產品系統存在安全漏洞(CVE-2019-9653)，攻擊者可繞過身分驗證於目標系統上執行任意程式碼。由於 NVR 系統之 handle_load_config.php 頁面缺少驗證與檢查機制，攻擊者可透過發送客製化惡意請求，利用此漏洞以管理者權限(root)遠端執行系統指令。 | | |
| 影響平台 | NUUO NVR 相關產品其韌體版本為 1.7.x 至 3.3.x 版本 | | |
| 影響等級 | 中 | | |
| 建議措施 | 目前京晨科技官方已有較新版本的韌體釋出，建議將韌體版本升級至最新版本：<br><br>1.使用官方提供之新版本韌體進行更新，下載連結：https://www.nuuo.com/DownloadMainpage.php<br><br>2.針對無法更新之 NVR 系統，請透過防護設備或系統內部設定限制存取來源，嚴格限制僅管理人員能夠存取系統之 handle_load_config.php 頁面，並禁止對該頁面發送任何系統指令與傳入特殊字元。 | | |
| 參考資料 | 1.https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9653<br><br>2.https://www.nuuo.com/DownloadMainpage.php | | |

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