

張貼日期：2019/06/06

【資安漏洞預警通知】京農科技(NUOO Inc.)網路監控錄影系統(Network Video Recorder, NVR)存在安全漏洞(CVE-2019-9653)

主旨：【資安漏洞預警通知】京農科技(NUOO 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:
 - NUOO 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NUOO NVR產品系統存在安全漏洞(CVE-2019-9653)允許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:
 - NUOO NVR相關產品其韌體版本為1.7.x 至 3.3.x版本
- 建議措施:
 - 目前京農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：
 1. 使用官方提供之新版本韌體進行更新，下載連結：<https://www.nuoo.com/DownloadMainpage.php>
 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>
 2. <https://www.nuoo.com/DownloadMainpage.php>

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:20190606_01

Last update: **2019/06/06 14:38**

