

張貼日期：2019/10/30

【資安漏洞預警】惡意音源檔案攻擊，請各單位注意防範

主旨：惡意音源檔案攻擊，請各單位注意防範

說明：

- 內容說明
 - 台灣電腦網路危機處理暨協調中心接獲國際情資，駭客利用WAV 音源檔案夾帶了惡意程式，迴避資安防禦機制，入侵終端系統執行惡意攻擊。
 - IOC資訊：https://cert.tanet.edu.tw/pdf/malicious_iocs.zip
- 影響平台: 所有能撥放wav音檔系統
- 建議措施: 根據IOC資訊，檢測終端系統檔案
- 參考資料:
 1. <https://www.virustotal.com/gui/file/595a54f0bbf297041ce259461ae8a12f37fb29e5180705eafb3668b4a491cecc/detection>
 2. <https://www.virustotal.com/gui/file/db043392816146bbe6e9f3fe669459fea52a82a77a033c86fd5bc2f4569839c9/detection>
 3. <https://www.virustotal.com/gui/file/a2923d838f2d301a7c4b46ac598a3f9c08358b763b1973b4b4c9a7c6ed8b6395/detection>
 4. <https://www.virustotal.com/gui/file/843cd23b0d32cb3a36b545b07787ac9da516d20db6504f9cdfa806d725d57f0/detection>
 5. <https://www.virustotal.com/gui/file/ed58fdb450d463b0fe3bbc6b9591203f6d51bf7a8dc00f9a03978cecd57822e1/detection>
 6. <https://www.virustotal.com/gui/file/da581a5507923f5b990fe5935a00931d8cd80215bf588abec425114025377bb1/detection>

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/ mailing:announcement:20191030_01

Last update: **2019/10/30 11:03**

