張貼日期：2022/08/09

【資安漏洞預警□VMware存在安全漏洞(CVE-2022-31656)□請儘速確認並進行更新

主旨□VMware存在安全漏洞(CVE-2022-31656)□攻擊者可藉此取得管理員權限，請儘速確認並進行更新

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202208-0403
  - VMware於8/2宣布修補旗下產品之高風險安全漏洞(CVE-2022-31656)□攻擊者若能透過網路存取VMware Workspace ONE Access□Identity Manager及vRealize Automation等3項服務，則可利用此漏洞繞過身分鑑別(Authentication Bypass)□進而取得管理員權限。
- 影響平台：
  - VMware Workspace ONE Access Appliance 21.08.0.0至21. 08. 0. 1版本
  - VMware Identity Manager Appliance & Connector 3.3.4至3. 3. 6版本
  - VMware Identity Manager Connector 19.03.0.1版本
- 建議措施：
  目前VMware官方已針對此漏洞釋出修復版本，請各機關可聯絡設備維護廠商或參考官方說明（https://kb.vmware.com/s/article/89096 ）之□Resolution□一節進行更新
- 參考資料：
  1. https://www.ithome.com.tw/news/152286
  2. https://kb.vmware.com/s/article/89096
  3. https://www.vmware.com/security/advisories/VMSA-2022-0021.html

—– 計算機與通訊中心
網路系統組 敬啟