**張貼日期：2019/05/14**

# [資安漏洞預警通知] Cisco ESC軟體存在安全漏洞(CVE-2019-1867)允許遠端攻擊者繞過認證機制取得管理者權限，請儘速確認並進行修正

主旨：[資安漏洞預警通知] Cisco ESC軟體存在安全漏洞(CVE-2019-1867)允許遠端攻擊者繞過認證機制取得管理者權限，請儘速確認並進行修正

- 內容說明:
  - Cisco Elastic Services Controller (ESC)是一款提升網路功能虛擬化(NFV)環境彈性的軟體。
  - 研究團隊發現Cisco ESC軟體的REST API存在安全漏洞(CVE-2019-1867)攻擊者可利用此漏洞，透過發送惡意請求，進而獲取管理者權限。
- 影響平台:
  - Cisco Elastic Services Controller 4.1至4.4 (含)版本，且啟用REST API
- 建議措施:
  - 目前Cisco官方已針對此弱點釋出修復版本，請各機關聯絡設備維護廠商或參考以下建議進行更新：
    1. 於ESC指令介面輸入esc_version指令，確認當前使用的ESC軟體版本。
    2. REST API預設為停用，於ESC指令介面輸入sudo netstat -tlnup | grep 8443|8080指令，可確認REST API是否啟用。
    3. 如使用受影響之ESC軟體版本，且啟用REST API時，請瀏覽Cisco官方更新網頁(http://www.cisco.com/cisco/software/navigator.html)，於Download Software頁面點擊Products→Cloud and Systems Management→Service Management and Orchestration→Elastic Services Controller將ESC軟體更新至4.5(含)以上版本。
- 參考資料:
  1. https://www.us-cert.gov/ncas/current-activity/2019/05/07/Cisco-Releases-Security-Update-Elastic-Services-Controller
  2. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190507-esc-authbypass

---

計算機與通訊中心
網路系統組 敬啟