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-2019-0054	發布時間	Tue May 14 09:36:42 CST 2019
事件類型	漏洞預警	發現時間	Thu May 09 00:00:00 CST 2019
警訊名稱	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		
影響等級	高		
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		

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