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-2018-0025	發布時間	Fri Mar 09 17:47:16 CST 2018
事件類型	漏洞預警	發現時間	Fri Mar 09 00:00:00 CST 2018
警訊名稱	Cisco 安全存取控制伺服器(Cisco Secure ACS)存在 Java 反序列化漏洞，允許未經授權的遠端攻擊者以 root 權限執行任意指令，請儘速確認並進行修正		
內容說明	Cisco 安全存取控制伺服器(Cisco Secure ACS)提供網路設備集中管理帳號密碼與權限管理之功能，網路管理人員連線至網路設備進行管理與設定時，可透過 Cisco 安全存取控制伺服器進行認證及取得授權指令，並留下稽核軌跡紀錄。 研究團隊發現 Cisco 安全存取控制伺服器存在 Java 反序列化(Deserialization)漏洞(CVE-2018-0147)，導致未經授權的遠端攻擊者可針對目標設備發送特製的 Java 序列化物件，進而造成遠端攻擊者可以 root 權限執行任意指令。		
影響平台	Cisco Secure ACS 5.8.0.32.8(含)以前的版本		
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，請各機關可聯絡設備維護廠商或參考以下建議進行更新： 1.於 Cisco Secure ACS 指令介面輸入「show version」指令確認當前使用的版本。 2.如使用受影響之 Cisco Secure ACS 版本，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 > Security > Network Visibility and Enforcement > Secure Access Control System > Secure Access Control System 5.8」，選擇 5.8.0.32.9 或以上版本進行更新。		
參考資料	1.https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs2 2.https://securitytracker.com/id/1040463		

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