

張貼日期: 2018/03/13

[資安漏洞預警通知] 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

主旨: 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

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。
- 影響平臺:
 - Cisco Secure ACS 5.8.0.32.8(含)以前的版本
- 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-ac52>
 2. <https://securitytracker.com/id/1040463>

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:20180313_01

Last update: 2018/03/13 09:28

