張貼日期：2018/04/03

［資安漏洞預警通知］資訊設備疑存在遠端程式碼執行漏洞

主旨：［資安漏洞預警通知］資訊設備疑存在遠端程式碼執行漏洞

說明：

- Cisco Smart Install提供網路交換器隨插即用配置和IOS Image 管理的功能，Cisco於2018年3月28日公布了該功能的漏洞(CVE-2018-0171)，允許未經身份驗證之攻擊者利用TCP 4786通訊埠，執行指令並控制該設備，造成受影響之設備發生阻斷服務。透過Shodan查詢，教育部網路與學術網路中存在近千台Cisco設備使用公開IP，並開啟TCP 4786通訊埠可遭存取利用。
- 影響平臺：
  1. Catalyst 4500 Supervisor Engines
  2. Catalyst 3850 Series
  3. Catalyst 3750 Series
  4. Catalyst 3650 Series
  5. Catalyst 3560 Series
  6. Catalyst 2960 Series
  7. Catalyst 2975 Series
  8. IE 2000
  9. IE 3000
  10. IE 3010
  11. IE 4000
  12. IE 4010
  13. IE 5000
  14. SM-ES2 SKUs
  15. SM-ES3 SKUs
  16. NME-16ES-1G-P
  17. SM-X-ES3 SKUs
- 建議措施：
  1. 盤點與檢視相關設備系統，確認設備是否受漏洞影響。若該設備為受影響之型號，請安裝最新之修補程式。
  2. 相關設備系統應置於實體防火牆設備後端並設置防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠，過濾內外部異常網路連線。若無使用Smart Install功能之需求，建議關閉該功能。
  3. 請開啟相關主機作業系統與應用程式日誌，並定期分析可疑行為（如：登入失敗、流量異常上升及非正常時間之登入行為）。
- 參考資料：
  1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2
  2. https://embedi.com/blog/cisco-smart-install-remote-code-execution/
  3. https://www.shodan.io/search?query=org%3ATANET+port%3A4786&page=1
  4. https://www.shodan.io/search?query=org%3Amoec+port%3A4786

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:20180403_02

Last update: **2018/04/03 10:09**