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-2018-0036	發布時間	Tue Apr 03 08:56:21 CST 2018
事件類型	漏洞預警	發現時間	Sat Mar 31 00:00:00 CST 2018
警訊名稱	Cisco IOS 與 IOS XE 軟體存在多個安全漏洞，允許遠端攻擊者執行任意程式碼或阻斷服務攻擊等，請儘速確認並進行修正		
內容說明	Cisco 官方於 3 月份的安全建議與警訊中，公告 Cisco IOS 與 Cisco IOS XE 等軟體存在多個安全漏洞，其中又以 Cisco IOS 與 Cisco IOS XE 中的智慧安裝(Smart Install)功能，所存在的緩衝區溢位漏洞(CVE-2018-0171)最為嚴重，Smart Install 功能可透過現有的作業系統映像檔部署交換機組態並提供組態備份之功能。 未經授權的遠端攻擊者可向受影響設備的 TCP Port 4786 發送特製的智慧安裝訊息(Smart Install Message)，進而造成設備重新加載，攻擊者亦可能在受害系統上執行任意程式碼，或造成阻斷服務攻擊等。		
影響平台	目前已知影響平台如下： Catalyst 4500 Supervisor Engines Catalyst 3850 Series Catalyst 3750 Series Catalyst 3650 Series Catalyst 3560 Series Catalyst 2960 Series Catalyst 2975 Series IE 2000 IE 3000		

	IE 3010 IE 4000 IE 4010 IE 5000 SM-ES2 SKUs SM-ES3 SKUs NME-16ES-1G-P SM-X-ES3 SKUs
影響等級	高
建議措施	1.利用 Cisco 官方提供的頁面進行版本確認，操作方式如下： a.查詢使用設備版本號，於設備系統指令頁面輸入指令「show version」。 b.至 Cisco 官方提供的頁面：https://tools.cisco.com/security/center/softwarechecker.x 左側選擇 method A。 c.選擇 IOS 或 IOS XE，並將版本號碼填寫至欄位，按下 continue。 d.進入步驟 2 後，點選第二個選項(只列出 3.28 安全性更新選項)，點擊 continue。 e.於頁面可檢視版本對應弱點，與弱點 First Fix 版本訊息，並洽設備供應商進行系統更新。 2.若無法立即更新，且無使用需求，建議關閉「Smart Install」功能。 a.查詢「Smart Install」狀態，於設備系統指令頁面輸入指令「show vstack config」。 b.於設備系統指令頁面輸入指令「no vstack」關閉「Smart Install」功能。 c.於對外防火牆關閉 TCP Port 4786，降低由外部來的攻擊威脅。
參考資料	1.https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-201

	80328-smi2 2.https://exchange.xforce.ibmcloud.com/vulnerabilities/140911 3.https://securitytracker.com/id/1040580 4.https://www.securityfocus.com/bid/103538 5.https://embedi.com/blog/cisco-smart-install-remote-code-execution/

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