國立成功大學 National Cheng Kung University

# NICS-ANA-2025-0000551 2025-10-29 【漏洞預警】Cisco IOS與IOS XE 軟體存在高風險安全漏洞(CVE-2025-20352)，請儘速確認並進行修補

國家資通安全研究院

漏洞/資安訊息警訊

| | | | |
|---|---|---|---|
| 發布編號 | NICS-ANA-2025-0000551 | 發布時間 | Tue Oct 28 17:58:13 CST 2025 |
| 事件類型 | 漏洞預警 | 發現時間 | Tue Oct 28 00:00:00 CST 2025 |
| 警訊名稱 | Cisco IOS與IOS XE 軟體存在高風險安全漏洞(CVE-2025-20352)，請儘速確認並進行修補 | | |
| 內容說明 | 研究人員發現Cisco IOS與IOS XE軟體之SNMP功能存在堆疊型緩衝區溢位(Stack-based Buffer Overflow)漏洞(CVE-2025-20352)。遠端攻擊者若擁有SNMPv1/v2c之唯讀community字串，或有效之SNMPv3帳號通行碼，可能利用該漏洞進行以下攻擊行為：<br><br>1.具備低權限之遠端攻擊者：可透過傳送特製SNMP封包，使執行Cisco IOS或Cisco IOS XE之設備重新啟動，造成阻斷服務(DoS)。<br><br>2.具備高權限(如privilege 15)之遠端攻擊者：可透過傳送特製SNMP封包，於Cisco IOS XE設備上，以root權限執行任意程式碼，進而取得系統控制權。<br><br>目前該漏洞已遭駭客利用，請儘速確認並進行修補。 | | |
| 影響平台 | Cisco IOS<br><br>Cisco IOS XE<br><br>詳細版本可參考官方公告中Fixed Software章節，該章節有提供影響版本確認選單，選擇產品並輸入版本號後，網站會顯示該產品之版本是否有受到影響。網址如下：<br><br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte#fs | | |
| 影響等級 | 高 | | |
| 建議措施 | 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：<br><br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte | | |
| 參考資料 | 1.https://nvd.nist.gov/vuln/detail/CVE-2025-20352<br><br>2.https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte | | |

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。

如果您對此通告內容有疑問或有關於此事件之建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 臺北市中正區延平南路143號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nics.nat.gov.tw