張貼日期：2023/10/23

【漏洞預警】Cisco IOS XE存在高風險安全漏洞(CVE-2023-20198)，請儘速參閱官方建議措施

- 主旨說明：Cisco IOS XE存在高風險安全漏洞(CVE-2023-20198)，允許遠端攻擊者在未經身分鑑別之情況下，取得受影響系統之控制權，請儘速參閱官方建議措施
- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202310-00000022，
  - 研究人員發現Cisco IOS XE之網頁介面存在高風險安全漏洞(CVE-2023-20198)，允許遠端攻擊者在未經身分鑑別之情況下，新增Level15之高權限帳號，進而利用此帳號控制受影響之系統。該漏洞目前已遭駭客利用，官方正積極修補中，後續更新請參考官網公告。
- 影響平台:
  - Cisco IOS XE若啟用網頁介面(Web UI)功能皆會受到影響
- 建議措施:
  - 目前Cisco官方尚未釋出更新程式，僅公告建議措施，請參考Cisco官方網頁之「Recommendations」一節，關閉HTTPServer功能或僅允許受信任設備進行HTTP/HTTPS連線，網址如下：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z#REC
- 參考資料:
  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
  2. https://nvd.nist.gov/vuln/detail/CVE-2023-20198
  3. https://arstechnica.com/security/2023/10/actively-exploited-cisco-0-day-with-maximum-10-severity-gives-full-network-control/
  4. https://www.darkreading.com/vulnerabilities-threats/critical-unpatched-cisco-zero-day-bug-active-exploit
  5. https://www.ithome.com.tw/news/159338

計算機與通訊中心
網路系統組 敬啟