

張貼日期：2026/10/05

【漏洞預警】Cisco ISE與ISE-PIC存在高風險安全漏洞(CVE-2026-20130、CVE-2026-20192、CVE-2026-20307、CVE-2026-76423及CVE-2026-76460)請儘速確認並進行修補

- 主旨說明：【漏洞預警】Cisco ISE與ISE-PIC存在高風險安全漏洞(CVE-2026-20130、CVE-2026-20192、CVE-2026-20307、CVE-2026-76423及CVE-2026-76460)請儘速確認並進行修補
- 內容說明：
 - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-200-202610-00000001
 - 研究人員發現Cisco ISE與ISE-PIC存在多項高風險安全漏洞(CVE-2026-20130、CVE-2026-20192、CVE-2026-20307、CVE-2026-76423及CVE-2026-76460)類型包含程式碼注入(Code Injection)、不當存取控制(Improper Access Control)、不安全之反序列化(Insecure Deserialization)及身分鑑別繞過(Authentication Bypass)其中CVE-2026-76460已遭駭客濫用，請儘速確認並進行修補。
 - CVE-2026-20130 未經身分鑑別之遠端攻擊者可藉由在傳遞至下游元件之輸出中，植入未經妥善處理之特殊元素，於受影響裝置執行任意程式碼。
 - CVE-2026-20192 未經身分鑑別之遠端攻擊者可繞過身分鑑別與授權限制，進而未授權存取受影響裝置。
 - CVE-2026-20307 已通過身分鑑別之遠端攻擊者可藉由向網頁管理介面傳送特製之Java序列化物件，於底層作業系統執行任意程式碼，並將權限提升至root。
 - CVE-2026-76423 未經身分鑑別之遠端攻擊者可藉由向對外開放之REST API連接埠傳送特製HTTP請求，以管理者權限讀取及變更ISE組態與身分資料。
 - CVE-2026-76460 未經身分鑑別之遠端攻擊者可藉由向存在缺陷之API端點傳送特製請求，繞過網頁管理介面之身分鑑別，進而未授權存取受影響裝置。
- 影響平台：
 - Cisco ISE與ISE-PIC 3.1至3.5版本
 - Cisco ISE與ISE-PIC 3.0(含)以前版本(已終止軟體維護)
- 建議措施：
 - 官方已針對漏洞釋出修補或更新，請參考官方說明進行處置，網址如下：
 - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-IS-E-ABP-VNSW7Tn5>
 - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-is-e-multi-hrP9jQSQ>
 - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-is-e-rce-se7bYU57>
 - <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>
- 參考資料：
 1. <https://nvd.nist.gov/vuln/detail/CVE-2026-20130>
 2. <https://nvd.nist.gov/vuln/detail/CVE-2026-20192>
 3. <https://nvd.nist.gov/vuln/detail/CVE-2026-20307>
 4. <https://nvd.nist.gov/vuln/detail/CVE-2026-76423>

5. <https://nvd.nist.gov/vuln/detail/CVE-2026-76460>
 6. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
 7. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-is-e-multi-hrP9jQSQ>
 8. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-is-e-rce-se7bYU57>
 9. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>
 10. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-notice-jfxK98ZP>
-

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/mailling:announcement:20261005_22



Last update: **2026/10/05 12:18**