[資安訊息警訊] 國家資通安全研究院（事件編號：NICS-ANA-2026-0000561)

# 國家資通安全研究院

# 漏洞/資安訊息警訊

| | | | |
|---|---|---|---|
| 發布編號 | NICS-ANA-2026-0000561 | 發布時間 | Fri Jun 26 16:03:14 CST 2026 |
| 事件類型 | 漏洞預警 | 發現時間 | Fri Jun 26 00:00:00 CST 2026 |
| 警訊名稱 | Cisco Identity Services Engine(ISE)存在高風險安全漏洞(CVE-2026-20181)，請儘速確認並進行修補 | | |
| 內容說明 | 研究人員發現 Cisco Identity Services Engine(ISE)與 ISE Passive Identity Connector(ISE-PIC)存在遠端程式碼執行(Remote Code Execution)漏洞(CVE-2026-20181)，已取得管理權限之遠端攻擊者可藉由發送特製 HTTP(S)請求，於設備上以 root 權限執行任意程式碼，請儘速確認並進行修補。 | | |
| 影響平台 | Cisco ISE/ISE-PIC 3.3(含)以前、3.4 及 3.5 版本 | | |
| 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-ise-multi-G5WP8vv#fs | | |
| 參考資料 | 1. https://nvd.nist.gov/vuln/detail/CVE-2026-20181<br><br>2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv | | |

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