[資安訊息警訊] 國家資通安全研究院（事件編號：NICS-ANA-2026-0000421)

國家資通安全研究院

漏洞/資安訊息警訊

發布編號	NICS-ANA-2026-0000421	發布時間	Fri May 15 16:23:15 CST 2026
事件類型	漏洞預警	發現時間	Fri May 15 00:00:00 CST 2026
警訊名稱	Ivanti Endpoint Manager(EPM)與 Endpoint Manager Mobile(EPMM)存在高風險安全漏洞(CVE-2026-5786、CVE-2026-5787 及 CVE-2026-8111)，請儘速確認並進行修補		
內容說明	研究人員發現 Endpoint Manager(EPM)與 Ivanti Endpoint Manager Mobile(EPMM)存在高風險安全漏洞(CVE-2026-5786、CVE-2026-5787 及 CVE-2026-8111)，類型分別為不當存取控制(Improper Access Control)、不當憑證驗證(Improper Certificate Validation)及 SQL 注入(SQL Injection)，請儘速確認並進行修補。 【CVE-2026-5786】 已通過身分鑑別之遠端攻擊者可取得管理者存取權限。 【CVE-2026-5787】 已通過身分鑑別之遠端攻擊者可冒充已註冊之 Sentry 主機，並取得有效 CA 簽章用戶端憑證。 【CVE-2026-8111】 已通過身分鑑別之遠端攻擊者可注入任意 SQL 指令進而執行任意程式碼。		
影響平台	【CVE-2026-5786 與 CVE-2026-5787】 Ivanti Endpoint Manager Mobile 12.6.1.1(不含)以前版本 Ivanti Endpoint Manager Mobile 12.7.0.1(不含)以前版本		

	Ivanti Endpoint Manager Mobile 12.8.0.1(不含)以前版本 【CVE-2026-8111】 Ivanti Endpoint Manager 2024 SU5(含)以前版本
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： https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-May-2026?language=en_US
參考資料	1. https://nvd.nist.gov/vuln/detail/CVE-2026-5786 2. https://nvd.nist.gov/vuln/detail/CVE-2026-5787 3. https://nvd.nist.gov/vuln/detail/CVE-2026-8111 4. https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US 5. https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-May-2026?language=en_US

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