[資安訊息警訊] 國家資通安全研究院（事件編號：NICS-ANA-2026-0000422)

國家資通安全研究院

漏洞/資安訊息警訊

發布編號	NICS-ANA-2026-0000422	發布時間	Fri May 15 16:23:16 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	Fortinet 多項產品存在高風險安全漏洞(CVE-2026-26083 與 CVE-2026-44277)，請儘速確認並進行修補		
內容說明	研究人員發現 Fortinet FortiSandbox、FortiSandbox Cloud、FortiSandbox PaaS 及 FortiAuthenticator 存在高風險安全漏洞(CVE-2026-26083 與 CVE-2026-44277) ，類型分別為缺乏授權(Missing Authorization)與不當存取控制(Improper Access Control)，未經身分鑑別之遠端攻擊者可透過發送特製請求執行未經授權之程式碼或指令，請儘速確認並進行修補。		
影響平台	【CVE-2026-26083】 FortiSandbox 4.4.0 至 4.4.8 版本 FortiSandbox 5.0.0 至 5.0.1 版本 FortiSandbox Cloud 5.0.2 至 5.0.5 版本 FortiSandbox Cloud 23 所有版本 FortiSandbox Cloud 24 所有版本 FortiSandbox PaaS 4.4.5 至 4.4.8 版本 FortiSandbox PaaS 5.0.0 至 5.0.1 版本 FortiSandbox PaaS 21.3 所有版本 FortiSandbox PaaS 21.4 所有版本 FortiSandbox PaaS 22.1 所有版本		

	FortiSandbox PaaS 22.2 所有版本 FortiSandbox PaaS 23.1 所有版本 FortiSandbox PaaS 23.3 所有版本 FortiSandbox PaaS 23.4 所有版本 【CVE-2026-44277】 FortiAuthenticator 6.5.0 至 6.5.6 版本 FortiAuthenticator 6.6.0 至 6.6.8 版本 FortiAuthenticator 8.0.0 版本 FortiAuthenticator 8.0.2 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://fortiguard.fortinet.com/psirt/FG-IR-26-128 https://fortiguard.fortinet.com/psirt/FG-IR-26-136
參考資料	1. https://nvd.nist.gov/vuln/detail/CVE-2026-26083 2. https://nvd.nist.gov/vuln/detail/CVE-2026-44277 3. https://fortiguard.fortinet.com/psirt/FG-IR-26-128 4. https://fortiguard.fortinet.com/psirt/FG-IR-26-136

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