教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026090409090505	發佈時間	2026-09-04 09:07:13
事故類型	ANA-漏洞預警	發現時間	2026-09-04 09:07:13
影響等級	中		

[主旨說明:]【漏洞預警】Zimbra Collaboration 存在高風險安全漏洞(CVE-2026-73570)，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-200-202609-00000003

研究人員發現 Zimbra Collaboration 存在作業系統指令注入(OS Command Injection)漏洞(CVE-2026-73570)，當系統安裝選用套件 zimbra-snmp 並啟用 SNMP 通知功能時，未經身分鑑別之遠端攻擊者可藉由傳送特製 SMTP 請求，以 Zimbra 使用者權限執行任意作業系統指令。該漏洞已遭駭客利用，請儘速確認並進行修補。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

Zimbra Collaboration 10.1.20(不含)以前版本

[建議措施:]

官方已針對漏洞釋出修補程式，請升級 Zimbra Collaboration 至 10.1.20(含)以後版本。 詳細說明請參考官方公告，網址如下：

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
[参考資料:] 1. https://nvd.nist.gov/vuln/detail/CVE-2026-73570 2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-73570 3. https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories