教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026091401095555	發佈時間	2026-09-14 13:49:56
事故類型	ANA-漏洞預警	發現時間	2026-09-14 13:49:56
影響等級	低		

[主旨說明:]【漏洞預警】MikroTik RouterOS 存在 3 個重大資安漏洞

[內容說明:]

轉發　台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202609-00000015

網路設備製造商 MikroTik 發布重大資安漏洞，路由器作業系統 RouterOS 存在 3 個重大資安漏洞。

CVE-2026-67276（CVSS 4.x：9.2），RouterOS 在將 SSH 驗證請求與授權使用者金鑰比對時，不會比較完整 RSA 公鑰，而是檢查金鑰類型和模數，若攻擊者得知授權的 RSA 模數且偽造有效簽名，在沒有私鑰的情況下以目標用戶的身分開啟 SSH 命令通道。

CVE-2026-86060（CVSS 4.x：9.2），RouterOS 的 SSH 登入路徑中存在一個參數處理漏洞，該漏洞涉及以停用字元開頭的使用者名，允許攻擊者更改受信任的 RouterOS 策略掩碼，從而導致權限提升。

CVE-2026-67277（CVSS 4.x：8.8），RouterOS 完成身份驗證之前接受一個「related」btest session connection，駭客可在未經身份驗證的用戶端可以利用此狀態啟動 IPv4 UDP 測試，可能重啟 RouterOS。

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:]

MikroTik RouterOS 7.24 至 7.24.2(不含)版本

MikroTik RouterOS 7.9 至 7.23.4(不含)版本

MikroTik RouterOS 6.0.0 至 6.49.21(不含)版本

[建議措施:]

請更新至以下版本： MikroTik RouterOS 7.25 beta3(含)之後版本、 MikroTik RouterOS 7.24.2(含)之後版本、 MikroTik RouterOS 7.23.4(含)之後版本、 MikroTik RouterOS 6.49.21(含)之後版本

[參考資料:]

1. https://www.twcert.org.tw/tw/cp-169-11197-4c916-1.html