

WebScreen 點不進 elevated 視窗根治：高權注入器

報告日期:2026-08-21 專案:SOCKET/StkAgent + StkWebScreen

一、訴求與現象

客戶透過 WebScreen 連遠端桌面,點「電腦管理」等視窗點不進去——滑鼠移得過去,但點下去沒反應甚至 lost focus。改用 TeamViewer 或 AnyDesk 則完全正常。

二、根因

Agent 當初為了「一台工作站只佔一條 SMB 連線」(Win10 20 條上限)改成未提權執行,實測完整性為 Medium。Windows 的 UIPI(使用者介面權限隔離)鐵律:低完整性程式不能對高完整性(elevated)視窗送 SendInput。電腦管理/登錄編輯器/工作管理員提權操作都是 High 完整性視窗,故 Medium 的 Agent 注入被系統丟棄。TeamViewer/AnyDesk 以 SYSTEM 服務注入(完整性最高)故不受限。與 DPI/多螢幕/座標無關。

三、解決方法

項目	內容
新增高權注入器	stk_hiinput.exe(C):移植 screenshot.c 的 DPI-immune 注入(AbsMove/PhysVDesk)。由排程 STK_HiInput(/r1 HIGHEST /it 互動使用者)以 High 完整性啟動。
純本機不佔 SMB	★只綁 127.0.0.1:9543、完全不連網路磁碟/relay → 提權但零網路 → 不佔任何 SMB 連線,維持一站一條的設計不破。這是本方案的關鍵。
Agent 轉發+備援	Agent 收 REMOTE_INPUT 先轉發 helper(懶連+失敗5秒節流);連不上才退回原本的直接注入 → 未更新站/helper 掛掉時行為與今日完全相同(fallback-safe)。
安裝與清除	install_agent :MAKE_TASKS 建 STK_HiInput 排程、:START_AGENT 啟動、:MODE_RETIRE 與 uninstall 清除;stk_updater/uploader 納入派送清單。

四、驗證(S004 端到端,全遠端)

測試	方法	結果
High 注入器基本能力	helper 以 High 啟動, Medium 客戶端連 9543 送鍵盤打進 elevated 記事本, 剪貼簿回讀	PASS(讀回 314159)
完整鏈路	relay→新 Agent→helper move 到 (700, 500), 本機讀游標	PASS(游標精準落點)
實際使用情境	relay 點擊經 High helper 打開 elevated 電腦管理的「動作」下拉選單, 截圖	PASS(下拉開啟)
負對照	Medium 注入同一 elevated 視窗	無反應(重現原始 bug)

五、踩坑與技術

項目	說明
EXEC 卡 handler	Agent(Medium)以 EXEC 跑「會自動提權的指令」(start compmgmt.msc)會卡住 EXEC 執行緒(既有行為, 非本案);測試改本機開視窗 + relay REMOTE_INPUT 注入繞開。
座標換算	注入座標=實體像素;agent 截圖 1920x1080 被檢視工具顯示縮成 960 要x2, 選單座標估錯會兩張都無下拉→先用閉環(move+讀游標)確認注入通, 再修座標。
bcc32 編 GUI exe	-c 產 obj, 再 ilink32 -aa(GUI 子系統) c0w32.obj + ws2_32.lib 連結。
PowerShell 5.1	讀 UTF-8 .ps1 中文會亂碼→測試腳本純 ASCII;& 在 -ArgumentList 需拆開。

六、部署與限制

項目	說明
部署	4 檔(stk_hiinput.exe / Stk_Agent.exe / install_agent.bat / uninstall_agent.bat)已上母版;隨 updater A/B + S00X_DEPLOY 派送(fallback-safe)。
啟用	★真正生效需 Commander 推 install_agent.bat /selfheal 建 STK_HiInput 排程並啟動 helper。

限制(待強化)	helper 掛掉目前無 watchdog 自動重拉(下次登入/selfheal 才起, 期間退回 Medium);RDS 多人主機模式的 helper 排程尚未涵蓋。
---------	--