星連VPN 開源協議：安全複審報告

繁體中文版 · 新報告 · 2026-11-17

結論：原 P-01 至 P-04 在本次固定來源與已測範圍內有修復證據。未建立新的可重現協議安全漏洞；有一項 Draft 4 相容性文件資訊事項及需保留的部署風險。這不是無漏洞或無日誌認證。

1. 評估範圍與版本

報告日期：2026-11-17（Asia/Shanghai）。這是重新取得原始碼後的新評估，保留 2026-11-13 舊報告；本報告的修復結論以以下完整 commit 為準。

項目	記錄
Protocol SHA	ddfd0d7a6ee4b74561dda16315493796899e92d6
App SHA	49a0a31b710b3b07bd90c459e3aebd4fd8a193e9
協議規格	Draft 4; wire byte 0x01; implementation 1.0.0-draft
App 版本	0.1.0+1; first-generation prototype
本報告來源	53 tracked files; 49 added/modified/deleted paths vs retained Nov 13 snapshot
來源清單	source_inventory.json

App 的 Go pseudo-version 與 protocol-revision.txt 均對應上述協議 SHA。兩個舊 commit 不存在於新遠端已取得的歷史中，因此比較採用保留的舊檔案快照並正規化 CRLF；不宣稱 Git 祖先關係。原始碼快照與逐檔 SHA-256 可供覆核。

此開源版本自述為第一代協議 / 原型 App；目前商用官方 App 與 SingLink 2.0 核心不在本次來源範圍。先前免費 / 付費 Windows 測評不等於本次來源或商用版本證明。本次未登入帳號、擷取使用者流量、修改 VPN / 代理 / 登錄檔，也未將報告發送或公開發布。

來源：README.md:8；README.md:5；core/go.mod:5；SPEC.md:3。

2. 方法、獨立性與證據等級

依使用者要求，由三個分開的 AI 代理進行協議審查、App 審查與反向交叉覆核，主代理整合並另行跑基準、模糊測試與 Linux 測試。這是不同審查路徑，並非獨立人類團隊、外部資安公司認證或形式化密碼學證明。原廠文件是待驗證的說法，沒有當成執行指令或通過證據。

證據分為：原始碼觀察、原廠測試重新執行、審查者新增控制、真正 OS API 元件測試，以及尚未完成的真機 / 生產環境驗收。測試通過不代表不存在漏洞。風險採定性分級，未指定未驗證的 CVSS 數字。

工具為 Go 1.27.4、Flutter 3.35.6 / Dart 3.9.2、govulncheck v1.9.0；實際命令、時間、環境、stdout、stderr 與退出碼見每個 evidence ID。Go 使用 local toolchain，未無聲切換下載版本。報告日期採本機時區；記錄中 ISO 時間保留其 UTC offset。

Linux 測試在 QEMU TCG 的 Alpine 3.22.8 / Linux 6.12.115 RAM-root 執行，無網卡、無主機資料夾分享、無主機磁碟、僅 guest loopback；不是正式伺服器部署。QEMU 下載 SHA-512 與 Alpine rootfs SHA-256 對照發布者資料，kernel 只記錄官方 HTTPS 來源與雜湊，未額外驗證獨立簽章。所有 guest 測試以 root 執行；不是非 root 部署驗證。使用了真正 Linux flock、rename、fsync 與子程序，但未模擬實體磁碟斷電或多主機共享儲存。

證據：ENV-LINUX-GUEST-RUN-R2；工具來源；交叉審查筆記。

威脅模型與涵蓋路徑

分別檢查可修改網路輸入的未認證對手、持有效 token 的濫用者、一般設定檔外洩、啟動 / 停止競態，以及 build / 原生函式庫信任面。節點 root / 同使用者惡意程式、完整簽署金鑰失陷不會被當成一般遠端攻擊等價情境。重點包括 parser / frame / AEAD / token / early data、重放 / 撤銷 / 地址政策、憑據遷移、FFI / FD 交接與 release gates。檔案總數是來源清冊，不代表逐行證明所有檔案、gVisor、Flutter、OS 或第三方依賴完全安全；審查集中在上述安全關鍵路徑。

3. 舊問題修復矩陣

「已修復」限於原始重現條件，不包含未測正式環境。先前本地報告只有四個協議問題；新原廠文件另提五個 third-party findings / P-05，不能反向歸為我們舊報告發現，也不能當作外部人類審計認證。

ID	狀態 / 測得行為	證據與界線
P-01	已修復：持久、原子防重放准入。	獨立同庫新 Server / 輪替測試及 Linux restart、並行子程序、突發退出通過；依賴共享狀態與支援檔案系統。
P-02	已修復：解析完整才發布撤銷名單，錯誤保留有效舊名單。	獨立 malformed/truncated 控制與 Linux 原廠回歸；未測正式控制面發布。
P-03	已修復指定 64:ff9b::/96 與 mapped IPv4 等價政策。	純政策及 Linux 控制；未測實際 NAT64 translator / 任意自訂翻譯前綴。
P-04	已修復過期 generation 發布與自身資源清理。	獨立 callback 控制與 Linux engine；Stop 仍非任意 callback 同步屏障，App 所有權另列 A-04。

P-01: 防重放

NewServer 不接受缺少 ReplayStore。通過驗證的 flight 先 CheckAndMark 原子提交才開目的連線；tag 以實際解密的靜態金鑰導出 HMAC，OldKeys 共用命名空間。保留到請求時間戳 +121 秒；容許向未來偏移時，首次接納後可能約需 241 秒保留。記錄錯誤、重複、滿容量及時間倒退均拒絕。外部 store 必須自行實現同等原子 / 耐久 / 時鐘合約。

singlink/server.go:140 · singlink/server.go:333 · singlink/replay.go:17 · singlink/replay_store.go:249

P-02: 撤銷名單

讀取 / 解析 / 發布序列化；有檔案與行長界線、末尾換行及 Scanner 錯誤處理。空檔 / 錯誤格式不能清除撤銷；清空必須明示 empty。發布新清單後關閉對應連線，准入註冊後再檢查一次。

singlink/revocation.go:14 · singlink/server.go:590 · singlink/server.go:405

P-03: 目的地址政策

先 unmap IPv4；對 well-known NAT64 同時檢查 IPv6 與內嵌 IPv4，自訂 deny 與 own/private 政策都涵蓋，快取目的亦重查。allowPrivate 是明示放寬，但不移除已設定 deny。網路特有翻譯前綴應額外設定。

singlink/policy_address.go:8 · singlink/policy_address.go:17

P-04: 生命週期

pending 啟動有取消與 generation；過期 finish 不發布 running，會呼叫該次 callback 傳回的清理。舊 watcher 不應停止新 client。callback 不接收 context，可延遲返回；因此 API 錯誤不代表從未取得資源。App 必須另行管理 FD 交接。

engine/lifecycle.go:18 · engine/lifecycle.go:31 · engine/lifecycle.go:78

控制：P-INDEPENDENT-RETEST; P-LINUX-SINGLINK; P-LINUX-ENGINE.

4. 新觀察：P-R01 / Draft 4 相容性文件

資訊事項，非加密漏洞。 IDENT 的作者字串從 SingLinkLabs 改為 SingLinkVPN，HKDF 演算法雖未變，輸入與導出的金鑰已變。SPEC 與 const.go 正確指出 Draft 3 / 4 不互通，但 remediation 文件第 20、207 行概括「wire identifiers / KDF 未變」，應限定其適用 commit 範圍。也可能原意僅指較早修復集合，故不判定為密碼學弱點。

應補充明確升級矩陣與錯版診斷，協調升級伺服器、App 和原生核心；保留精確 IDENT，不新增明文後備。wireVersion 仍為 1，不應據此推論相容。

SPEC.md:3 · singlink/const.go:45 · docs/SECURITY-REMEDIATION.md:20 · docs/SECURITY-REMEDIATION.md:207

5. 密碼學、明文與信任邊界

目前來源使用 32-byte 方向性 traffic key 建立 AES-GCM，因此本次應記為 **AES-256-GCM**，不是 AES-128。審查者控制驗證方向金鑰不同且為 32 bytes；自產 first-flight 明文標記未出現在序列化密文，正控制可解密，修改 AEAD 與已簽署能力資料均遭拒絕。這些是程式內序列化 / 解密測試，沒有執行封包擷取，亦非密碼破解難度證明。

設計結合 X25519 與 ML-KEM-768，仍屬自訂協議。第一個 flight 的保密性依賴靜態伺服器金鑰；第一個 flight 不具完整前向保密，first flight 之後的流量另混入 ephemeral-ephemeral X25519，設計提供經典攻擊者模型下的前向保密；靜態 KEM 金鑰日後遭入侵時仍不能主張後量子前向保密。應保留規格明示的限制，不能用「有後量子元件」取代完整分析。

應用程式本來就會在端點處理明文；VPN 節點解封裝後，非 HTTPS 等目的流量也可能是明文。內層 AES-256 不證明伺服器不記錄內容、營運日誌為零、所有 App 都走 VPN，或任一日本商用節點採用同一版本。外層 TLS / 憑證驗證、raw TCP 與 insecure 模式需各自評估；App 的明示警告不能被概括「已加密」介面取代。

來源：singlink/frame.go:30 · singlink/handshake.go:110 · singlink/handshake.go:156 · singlink/const.go:50；控制：P-INDEPENDENT-CRYPTO-EARLY。

6. 持久狀態、隱私與營運殘餘風險

FileReplayStore 使用穩定 .lock、私有目錄 / 檔案 / owner 檢查、檔案 fsync、同目錄 rename 與目錄 fsync。新狀態須明示 replay-init；一般啟動不會悄悄重建遺失或損壞檔。所有接納同一金鑰的程序必須分享命名空間；不得在舊金鑰仍有效時清空、回滾、刪除 lock 或還原舊備份。檔內 watermark 不能辨識整份自身狀態被回滾。systemd stable User 與 StateDirectory 設定符合來源合約，但沒有啟動正式 systemd 服務驗證。

狀態保存 keyed opaque tag、各 tag 到期時間和全域時鐘 watermark；不含原始 flight、帳號、IP、URL 或 payload 欄位，但仍有短期活動 / 時間資料。HMAC 降低未持有金鑰者直接匹配 tag 的能力，不代表時間關聯不可能。Serve 執行時每 30 秒 GC；停止節點仍留快照。邏輯刪除 / rename 不代表備份、舊區塊已安全抹除。不能據此發「零日誌」證書。

每次准入會在鎖下讀取 / 排序 / 重寫有界快照。預設 65,536 marks，上限 1,048,576；滿時拒絕以保存防重放性。有效 token 但能力遭拒的 flight 仍可先消耗 store 資源。審查者以 3-slot 記憶體控制，示範一個准許加兩個能力拒絕請求填滿後，另一有效 subject 也遭拒。這是文件已揭示的認證後容量風險，未對真實預設容量或正式節點發動耗盡攻擊。應測正式儲存效能、限制認證後 admission 速率、監測容量；不可透過提早淘汰未到期 marks 換速度。

singlink/replay_store.go:21 · singlink/replay_lock_unix.go:15 · singlink/replay_store.go:188 · singlink/server.go:258 · docs/SECURITY-REMEDIATION.md:90 · deploy/singlink.service:16

7. 實測數據

證據 ID	結果	類型
P-LINUX-SINGLINK	61 passed; exit 0	Linux 原廠原始套件
P-LINUX-ENGINE	6 passed; exit 0	Linux 原廠原始套件
P-LINUX-SOCKS5	4 passed; exit 0	Linux 原廠原始套件
P-LINUX-CLI	1 passed; exit 0	Linux 原廠原始套件
P-INDEPENDENT-RETEST	6 passed; exit 0	新增審查者控制
P-INDEPENDENT-CRYPTO-EARLY	4 passed; exit 0	新增審查者控制

Linux 四組協議套件合計 72 個頂層測試通過；另有 10 個新增審查者頂層控制，不能當成 82 個互不重疊的完整安全情境。Linux guest 全程 74.391 秒，含 App tunnel。singlink 套件含真正子程序並行與程序退出測試；退出 fixture 是 CheckAndMark 提交成功後 os.Exit(0)，未在 write / fsync 中途注入 SIGKILL，也不是斷電測試。

套件	執行 coverage / statements
singlink	82.80% (1261/1523)
engine	52.44% (86/164)
socks5	75.78% (244/322)
cmd/singlink	0.00% (0/258)

Coverage 是已插樁套件 statements，不是漏洞檢出率；CLI 通過的控制未覆蓋其主程式 statements，不可宣稱完整 CLI coverage。

目標	最終 elapsed	executions	new interesting
P-FuzzDecodeAddr	20 s	576,239	7
P-FuzzParseHeader	20 s	483,215	15
P-FuzzParseToken	20 s	679,330	3
P-FuzzParseLink	21 s	3,258	3
P-FuzzParseFirstFlight	21 s	3,831	1
P-FuzzReadFrame	20 s	712,716	7

六個目標各指定 20 秒、兩個 worker；最終輸出約 20-21 秒，合計 **2,458,589 executions**，全部退出 0。首次編譯另耗時，new interesting 指新增 coverage corpus，並非漏洞。未發現 crash 不代表長時間 fuzz 一定無問題。

Windows / Linux 的 go vet 與 govulncheck 均退出 0，無 finding 事件；govulncheck 是 source symbol 掃描，資料庫 last-modified 為 2026-11-11T02:51:11Z。協議 module 只有標準庫。零 finding 不涵蓋未知漏洞、設計錯誤或任意商用 binary。

P-VET-WINDOWS; P-VET-LINUX; P-VULN-WINDOWS; P-VULN-LINUX; P-MODULES

8. 失敗、限制與未執行項目

Windows 原始協議 baseline 退出 1：29 pass / 43 fail，多數 fixture 需要 Unix-only FileReplayStore，Windows 按設計 fail closed。它們不是 43 個已確認漏洞，也不能寫成全部通過。新增記憶體 adapter 只在審查者控制使用，絕不建議部署；後續 Linux 已跑原始持久後端。最初 QEMU 因 Windows 中文路徑無法找 BIOS；改 ASCII 暫存路徑後成功，失敗記錄保留。

本次沒有 race detector 成功執行證據、實體斷電、NFS / 多主機、正式 key custody / 控制面、真實 NAT64、macOS 後端、真實端到端商用服務測試。審查者 callback / first-flight 控制使用合成金鑰與 loopback。密碼學 review 非形式化證明。

P-BASELINE-WINDOWS; ENV-LINUX-GUEST-RUN

9. 建議處理順序與結案標準

1. 發布前修正 Draft 4 文件範圍，驗證實際 client / server / FFI 版本配對與無降級；同時處理 App 報告 A-04 的 FD 所有權合約。

2. 在正式同類 Unix 儲存與非 root 身分驗證 crash / restart / 輪替 / 容量 / 時鐘倒退；另做實體斷電與備份還原演練、共享 store 多主機合約及正式 admission 效能測量。不可把本次 RAM-root 當成上述結果。

3. 以相容原生環境執行 race detector、持續 fuzz / 長時間壓力測試、實際 NAT64 與撤銷控制面驗收；Windows 若作 node 需提供受支援 store。

4. 持續保留原始測試失敗與修正紀錄。原廠 APFS 效能數字、內部 31 findings 及 third-party 字樣均不是本次測量 / 認證。

本次審查工作已在上述明示範圍完成；這些是發布與營運驗收條件，不是已執行結果。沒有修改產品程式碼。不得將本結論改寫為「所有版本全面安全」、「沒有明文」或「證實伺服器不記錄」。

10. 證據包與重現說明

新報告、英文版與繁體版各自獨立，finding ID、commit、數字及限制對照一致。HTML / Markdown 是可編輯版；PDF 是閱讀版。入口為 START_HERE.html，完整檢查矩陣見 check_summary.json。

公開交付包只含本次報告、公開來源快照 / LICENSE / NOTICE、合成測試、測試結果與差異圖；不含帳號、付費憑據、個人瀏覽封包、工具快取或正式簽署金鑰。下載依賴時僅向官方 / 套件來源請求公開材料；OSV 只接收套件名與版本。這不等同聲稱測試全程完全離線：只有 Linux guest 無外部網路。

本機保留原始紀錄；分享包對本機使用者 / 工作目錄路徑做一致替換，redactions.json 記錄來源與分享檔雜湊。sources 逐檔 bytes 保持不變，SHA256SUMS.txt 驗證交付包內容。工具鏈、QEMU / SDK / module cache 不打包，避免把第三方工具重發與證據混在一起。重跑需先準備指定工具與相鄰 protocol checkout，並依 README_REPRODUCE.md 設定路徑；並非任意電腦一鍵可跑。

原始測試命令與退出碼清單：

ID	Exit	備註
P-BASELINE-WINDOWS	1	需讀取範圍 / 失敗原因
P-BUILD-LINUX-CLI	0	限定檢查通過
P-BUILD-LINUX-ENGINE	0	限定檢查通過
P-BUILD-LINUX-SINGLINK	0	限定檢查通過
P-BUILD-LINUX-SOCKS5	0	限定檢查通過
P-FuzzDecodeAddr	0	限定檢查通過

ID	Exit	備註
P-FuzzParseFirstFlight	0	限定檢查通過
P-FuzzParseHeader	0	限定檢查通過
P-FuzzParseLink	0	限定檢查通過
P-FuzzParseToken	0	限定檢查通過
P-FuzzReadFrame	0	限定檢查通過
P-INDEPENDENT-CRYPTO-EARLY	0	限定檢查通過
P-INDEPENDENT-RETEST	0	限定檢查通過
P-LINUX-CLI	0	限定檢查通過
P-LINUX-ENGINE	0	限定檢查通過
P-LINUX-SINGLINK	0	限定檢查通過
P-LINUX-SOCKS5	0	限定檢查通過
P-MODULES	0	限定檢查通過
P-VET-LINUX	0	限定檢查通過
P-VET-WINDOWS	0	限定檢查通過
P-VULN-LINUX	0	限定檢查通過
P-VULN-WINDOWS	0	限定檢查通過

再發布與署名

附帶來源的 LICENSE / NOTICE 保留原作者 SingLinkVPN 的署名要求；法律適用範圍未在本次做獨立法律鑑定。報告作者為受使用者委託的 AI 輔助評估；不使用原廠「third-party audit」措辭替本次背書。公開前請維持完整範圍、版本、殘餘問題與證據連結。