

ANTHROPIC CYBER VERIFICATION PROGRAM (CVP) - APPEALS & ELIGIBILITY DOSSIER

=====

Applicant Name: Serhii Shunko
Account Email: cc.simply.spolit@gmail.com
Organization UUID: c4ebb284-8fa8-4c0b-95fb-9cf6e36fc24b
Identity Status: pass_011Cfqc1KQAujYVncduA6dDL (VERIFICATION_TYPE_TAF_CYBER_IDV: VERIFIED)
Verification Portal: <https://ccsimplyspolit.github.io/>
GitHub (only account): <https://github.com/ccsimplyspolit>
HackerOne / Bugcrowd: <https://hackerone.com/sshunko> | <https://bugcrowd.com/h/sshunko>
LinkedIn / ORCID iD: <https://www.linkedin.com/in/sshunko/> | <https://orcid.org/0009-0002-4183-0361>
CERN / Zenodo DOIs: 10.5281/zenodo.23641037 | 10.5281/zenodo.23640494 | 10.5281/zenodo.23640496

1. SUMMARY OF DEFENSIVE RESEARCH & REASON FOR APPEAL

I am an independent systems and binary security researcher auditing open-source C/C++ network/media parsers, embeddable bytecode VMs, and AI/MCP server infrastructure under Coordinated Vulnerability Disclosure (CVD). My identity is verified via Persona (VERIFICATION_TYPE_TAF_CYBER_IDV). This dossier documents 8 maintainer-acknowledged vulnerability disclosures, 58 private GHSA reports in maintainer triage, 4 active HackerOne disclosures, and 3 CERN/Zenodo DOIs to satisfy CVP Defense Access eligibility.

2. MAINTAINER-ACKNOWLEDGED VULNERABILITY DISCLOSURES (8 TOTAL)

-
- 1) GHSA-g52w-56c5-674f | SalesforceCommerceCloud/b2c-developer-tooling (High 7.1, CWE-22)
* Scope: Path Containment Omission in Services.resolveWithProjectDirectory()
* Status: Officially PUBLISHED by Salesforce (2026-10-28); Fix PR #828 Merged.
 - 2) HackerOne #4148578 | brave/ai-gateway (Brave Software Bug Bounty Program)
* Scope: Streaming Tool-Call Alignment Bypass & Attachment Extraction Bug
* Status: Closed as Informative 2026-10-27; \$50.00 USD bounty awarded.
 - 3) GHSA-pvw7-7j8c-qx96 | opensensor/lightNVR (High 8.1, CWE-285 / CWE-416)
* Scope: Auth Bypass via Query-Param Truncation in api_handlers_go2rtc_proxy.c
* Status: Accepted into Draft GHSA by @matteius & Patched in v0.44.3 (507bce1c0715).
 - 4) GHSA-qm7x-j9xp-x3gv | czlonkowski/n8n-mcp (CWE-918 / CWE-184)
* Scope: SSRF Protection Skipped Trailing-Dot & *.localhost in validateUrlSync
* Status: Accepted into Draft GHSA & Patched in v2.99.2 (commit a49dfb4).
 - 5) GHSA-cr23-59mg-h2rc | bacnet-stack/bacnet-stack (High 8.2, CWE-835 / CWE-125)
* Scope: Negative Decode Length Infinite Loop & OOB Read in Calendar_Write_Property
* Status: Accepted into Draft GHSA by @skarg; Upstream Fix PR #1595 Open.
 - 6) GHSA-6hh9-gpj4-cr69 | moonlight-stream/moonlight-common-c (CWE-125 / CWE-908)
* Scope: Missing IDX_DS_ADAPTIVE_TRIGGERS Sentinel in src/ControlStream.c
* Status: Fix PR #168 Merged into master by @cgutman on 2026-10-26T22:46:49Z.
 - 7) GHSA-w6v4-9j58-rv79 | FreeRADIUS/freeradius-server (Critical 9.8, CWE-125 / CWE-345)
* Scope: EAP-FAST Nested TLV OOB Read & Crypto-Binding Bypass in rlm_eap_fast.c
* Status: Patched on master by @alandekok (commits 1ef1b499f1 & 1c7661e1bd).
 - 8) GHSA-x9vx-8c8r-c57x | Infomaniak/mcp-server-kchat (Medium 5.4, CWE-22 / CWE-88)
* Scope: Unvalidated username Path Traversal in getUserByUsername() (kchat-client.ts)
* Status: Fix PR #70 Merged by @L3o-pold in v1.1.1 (commit 5ed2728f5a).

3. ACTIVE PRIVATE DISCLOSURES IN UPSTREAM MAINTAINER TRIAGE

-
- * GitHub Private Vulnerability Reporting (58 Advisories in Triage, 29 Oct):
58 private GSAs (state: triage) across C/C++ protocol/media parsers and AI/MCP servers, each paired with an ASan/runtime reproducer and patch.
 - * Active HackerOne Disclosures in Upstream Triage (4 Reports, state: new):
 - #4148863 (Ruby IBB / ruby/ruby Onigmo regex engine; @makenowjust joined)
 - #4145362 (Nebius AI VDP: nebius/mcp-server & contree-mcp CLI flag bypass)
 - #4145363 (PagerDuty VDP: rundeck/mcp cross-origin token exfiltration/SSRF)
 - #4145745 (PagerDuty VDP: rundeck/rundec JobFileRecord path traversal)
 - * Bugcrowd Private Programs: Active researcher (@sshunko), including Cohere.

4. PUBLISHED OPEN-SOURCE SECURITY TOOLING (CERN / ZENODO DOIs)

-
- * protobuf-bounds-auditor (<https://doi.org/10.5281/zenodo.23641037>): Static .proto analyzer (CWE-1284/20/400) with SARIF v2.1.0 & DEFINE_PROTO_FUZZER.
 - * cs-telemetry-internals (<https://doi.org/10.5281/zenodo.23640494>): Source 2 protobuf wire bounds auditing & relocation-masked PE32+ integrity analyzer.
 - * cardinal-engine-integrity (<https://doi.org/10.5281/zenodo.23640496>): PE32+ section integrity, IAT boundary auditor & 4,423-function lockstep audit.