SICHERHEITS-AUDIT — RUNDE 9 (RELEASE)

NetMon Roots v1.1.19

Code Security Review — finaler Release-Stand — Juli 2026

Datum	18. Juli 2026
Analysierte Version	v1.1.19 — finaler Release-Stand
Schwerpunkt	Killswitch-Reconcile, DNS-Recovery, Update-Check, deb-Skripte, Release-Signatur
Kritische Findings	0
Hohe Findings	0
Mittlere Findings	2 (beide behoben & verifiziert)
Haertungen umgesetzt	2 + neue Regressionstests
Release-Signatur (minisign)	gueltig verifiziert
Regressionstests	253 + 80 Tests, sicherheitsrelevante alle gruen
Analysewerkzeug	Claude Fable 5 (Anthropic)
Projektverantwortlicher	Sven Froehlich

0 KRITISCHE — 0 HOHE — 2 MITTLERE FINDINGS (BEIDE UMGESETZT & VERIFIZIERT)

1. Zusammenfassung

Die neunte Sicherheitsanalyse pruefte erstmals den finalen Release-Stand v1.1.19 statt eines Zwischenstands. Schwerpunkte: der VPN/UFW-Killswitch-Reconcile, die DNS-Startup-Recovery, der In-App-Update-Check, die Debian-Maintainer-Skripte (Install/Deinstall als root) und der komplette Release-Verifikationspfad (SHA256SUMS + minisign). Die Release-Artefakte wurden empirisch verifiziert: sha256sum -c bestaetigt alle drei Dateien, und die minisign-Signatur der SHA256SUMS ist gegen den gepinnten Public Key gueltig.

Anders als in den Vorrunden wurden zwei belastbare Schwachstellen mittleren Schweregrads bestaetigt (Validierung je Konfidenz 8/10). Beide wurden direkt umgesetzt, mit Regressionstests abgesichert und verifiziert. Keine kritischen oder hohen, keine klar remote-ausnutzbaren RCE-Befunde.

F1 (MEDIUM, behoben): Der In-App-Update-Check uebernahm die download_url aus der per HTTPS geladenen latest-version.json ungeprueft und uebergab sie beim Oeffnen des Ueber-Dialogs ohne weiteren Klick an xdg-open — ohne die http/https-Allowlist, die an vergleichbaren Stellen (Secure-Browser-fetch_url, Radio-Logo) bereits existiert. Ein kompromittierter Server/CDN haette so eine file://- oder Custom-Scheme-URL oder eine Phishing-Seite an den registrierten Desktop-Handler weiterreichen koennen (kein RCE — Listenform-Popen). Gehaertet: _open_url_with_xdg_open() erzwingt jetzt http/https; _is_trusted_update_url() beschraenkt die automatisch geoeffnete URL zusaetzlich auf die netmonroots.com-Domain und faellt sonst auf die fest konfigurierte Download-Seite zurueck.

F2 (MEDIUM, behoben): recover_firewall_after_killswitch_failure() setzte die Firewall bedingungslos auf 'ufw default allow outgoing' und wurde in drei fruehen Fehlerpfaden von vpn_switch() aufgerufen (leeres Ziel, nicht aufloesbares Runtime-Profil, WG-Cleanup-Fehler) — ohne zu pruefen, ob der Killswitch bewusst aktiv war. Ein fehlgeschlagener Slot-Wechsel bei aktivem Killswitch konnte so die deny-outgoing-Garantie still aufheben und Klartext-Traffic freigeben — ein Fail-Open in einer Kontrolle, deren Zweck Fail-Closed ist. Gehaertet: die drei Stellen nutzen jetzt _recover_firewall_preserving_killswitch(), das bei aktivem Killswitch die deny-outgoing-Policy per idempotentem _killswitch_on_sync() erhaelt und nur ohne aktiven Killswitch auf allow-outgoing zurueckgesetzt.

Ergaenzend: Die Release-Signaturkette ist technisch dicht, aber die minisign-Vollpruefung ist auf der Downloadseite nur als optionaler Zusatz dargestellt — Empfehlung, sie als Standardweg hervorzuheben (Doku/UX, keine Code-Luecke). Das postinst biegt aktive NM-DNS bei der Installation auf 8.8.8.8 um (Vorzustand gesichert, in prerm restauriert) — funktional sauber, aber fuer ein Privacy-Tool eine Policy-Frage (Opt-in empfohlen); kein ausnutzbarer Befund. Die Kindersicherung bleibt als bewusste Design-Entscheidung dokumentiert. Alle Runde-7/8-Haertungen sind intakt; Versionskonsistenz (App, deb, Site, latest-version.json) ist durchgaengig 1.1.19.

2. Methodik

Phase 1 - Release-Recon & Signaturpruefung

Verifikation der Artefakte: sha256sum -c SHA256SUMS (alle drei OK), minisign -V gegen den gepinnten Public Key (Signatur gueltig). Extraktion und Review der .deb-Maintainer-Skripte (postinst/prerm). Versionskonsistenz-Abgleich ueber App, deb-control, latest-version.json und Download-Seiten.

Phase 2 - Kandidaten-Analyse

Ein Analyse-Sub-Agent verfolgte Datenfluesse von Fremdeingaben (Update-/API-Antworten, VPN-Profil-/Slot-Daten, Install-Zeit-Zustand) bis zu privilegierten Senken (ufw/nmcli/wg-quick, xdg-open,

root-cp/chown). 5 Kandidaten identifiziert.

Phase 3 - False-Positive-Validierung

Die zwei belastbaren Kandidaten wurden von je einem eigenen Validierungs-Sub-Agenten gegengeprueft (beide Konfidenz 8/10, MEDIUM). Drei weitere Kandidaten (postinst-DNS-Policy, State-Datei-Parsing, root-Symlink-chown) lagen als Policy-/Grenzfall unter der Schwelle und sind nicht ausnutzbar im Threat Model.

Phase 4 - Haertung & Regressionscheck

Beide MEDIUM-Findings wurden umgesetzt, mit fuenf neuen Regressionstests abgesichert und verifiziert. Suiten erneut ausgefuehrt: Killswitch/VPN/DNS/Firewall (253) und Diagnostik/Update-Check (80) — alle sicherheitsrelevanten Tests gruen.

3. Bestaetigte Findings

F1 — Update-Check oeffnet server-gelieferte URL ohne Schema-Allowlist [MEDIUM, Konfidenz 8/10, behoben]

`netmon/app.py — _fetch_latest_release_info() / check_about_latest_version() / _open_url_with_xdg_open().`

Der In-App-Update-Check laedt latest-version.json per HTTPS und uebernimmt die download_url daraus ungeprueft. Wird beim Oeffnen des Ueber-Dialogs eine neuere Version erkannt, wird diese URL ohne weiteren Klick an xdg-open uebergeben — ohne Schema-/Host-Pruefung, obwohl dieselbe http/https-Allowlist an vergleichbaren Stellen (fetch_url, _station_logo_url) bereits existiert. Ein kompromittierter Server/CDN (im Threat Model enthalten) kann eine download_url mit beliebigem Schema (file://, vnc://) oder eine Phishing-Seite liefern, die xdg-open an den registrierten Desktop-Handler weiterreicht. Kein direktes RCE (Listenform-Popen, keine Shell-Injection), aber zuverlaessig fuer Phishing und situativ zum Ansteuern eines Scheme-Handlers.

Behebung: Gehaertet & verifiziert: _open_url_with_xdg_open() begrenzt Ziel-URLs auf http/https (deckt alle Aufrufer ab); _is_trusted_update_url() laesst nur eine netmonroots.com-URL automatisch oeffnen und faellt sonst auf die fest konfigurierte Download-Seite zurueck. Mit Regressionstests abgesichert.

F2 — Killswitch-Fail-Open in fruehen VPN-Slot-Wechsel-Fehlerpfaden [MEDIUM, Konfidenz 8/10, behoben]

`netmon/features/vpn_controller.py — vpn_switch(); netmon/features/firewall_controller.py — recover_firewall_after_killswitch_failure().`

recover_firewall_after_killswitch_failure() setzt die Firewall bedingungslos auf 'ufw default allow outgoing'. Sie wurde in drei fruehen Fehlerpfaden von vpn_switch() aufgerufen (leeres Ziel, nicht aufloesbares Runtime-Profil, WG-Cleanup-Fehler) — ohne zu pruefen, ob der Killswitch bewusst aktiv war. Hatte der Nutzer Killswitch AN + VPN aktiv und waehlte einen Slot, dessen Profil geloescht/umbenannt wurde oder dessen IPv4-Runtime-Kopie fehlt, brach vpn_switch() frueh ab und die deny-outgoing-Garantie wurde still auf allow zurueckgesetzt — Klartext-Traffic konnte das System verlassen, obwohl der Nutzer Killswitch-Schutz erwartete. Ein Fail-Open in einer Kontrolle, deren einziger Zweck Fail-Closed ist.

Behebung: Gehaertet & verifiziert: die drei Aufrufstellen nutzen jetzt _recover_firewall_preserving_killswitch(). War der Killswitch aktiv (killswitch_is_on(), ausgewertet vor jeder Zustandsaenderung), wird die deny-outgoing-Policy per idempotentem _killswitch_on_sync() erhalten statt geoeffnet; nur ohne aktiven Killswitch wird wie bisher auf allow-outgoing zurueckgesetzt, damit sich der Nutzer nicht aussperrt. Mit Regressionstests abgesichert.

4. Release-Verifikation & weitere Beobachtungen

Release-Signaturkette technisch dicht — Empfehlung zur Sichtbarkeit

SHA256SUMS deckt alle drei Artefakte korrekt ab (sha256sum -c OK) und ist per minisign signiert; die Signatur wurde gegen den gepinnten Public Key gueltig verifiziert. Das Verifier-Skript prueft jedoch nur die Hashes, und die prominente 'Schnellpruefung' auf der Downloadseite empfiehlt ebenfalls nur sha256sum -c — ein MitM, der .deb UND SHA256SUMS gemeinsam ersetzt, bestuende diesen Schnellcheck. Empfehlung (Doku/UX, keine Code-Luecke): die minisign-Vollpruefung als empfohlenen Standardweg hervorheben statt als optionalen 'falls signiert'-Zusatz.

Kindersicherung — weiterhin bewusste Design-Entscheidung

Die PBKDF2-gestuetzte Kindersicherung im Secure-Browser bleibt wie in Runde 8 dokumentiert: Alltagshuerde gegen Gelegenheitszugriff im selben Konto, keine harte Grenze gegen technisch versierte Nutzer mit Kontozugriff. Keine Codeaenderung, unveraendert gueltig.

postinst setzt aktive NM-DNS auf 8.8.8.8 — Policy-Hinweis

Das root-postinst biegt aktive NetworkManager-Verbindungen bei der Installation auf ipv4.dns 8.8.8.8 um (Vorzustand gesichert, in prerm restauriert). Funktional sauber und ohne ausnutzbaren Befund (State-Datei 0600 root, Argumentlisten-Aufrufe, keine Injection), aber fuer ein Privacy-Tool eine ueberraschende Richtung. Empfehlung: Opt-in statt hart verdrahtetem Public-Resolver. Als Design-Entscheidung des Projektverantwortlichen offen — keine Codeaenderung in dieser Runde.

5. Umgesetzte Haertungen (Runde 9)

Schema-Allowlist + Host-Pin fuer die Update-URL — app.py

_open_url_with_xdg_open() laesst nur noch http/https zu; _is_trusted_update_url() beschraenkt die automatisch geoeffnete Update-URL zusaetzlich auf die netmonroots.com-Domain.

Killswitch-erhaltender Recover-Pfad — vpn_controller.py / firewall_controller.py

_recover_firewall_preserving_killswitch() haelt die deny-outgoing-Policy bei aktivem Killswitch aufrecht (idempotenter Re-Sync), statt sie bei einem fehlgeschlagenen Slot-Wechsel still zu oeffnen.

Neue Regressionstests — 5 Tests

test_netmon_diagnostics.py (Update-URL-Allowlist / Host-Pin) und test_netmon_killswitch.py (Killswitch-erhaltendes Recover-Verhalten). Sicherheitsrelevante Suiten (253 + 80 Tests) sind gruen.

6. Geprüfte Sicherheitskategorien

Kategorie	Ergebnis
Sicherheitskontroll-Umgehung (Killswitch Fail-Open)	**F2 -> behoben (fail-closed)**
Unvalidierte Fremd-URL an Desktop-Handler (xdg-open)	**F1 -> behoben (Allowlist+Host-Pin)**
Command-/Argument-Injection (ufw/nmcli/wg-quick, subprocess)	**Kein Finding (list-form)**
DNS-Startup-Recovery (privilegierte nmcli/resolvectl)	**Kein Finding (validiert, fail-safe)**
Debian-Maintainer-Skripte (root cp/chown, State-Parsing)	**Kein ausnutzbarer Befund**
Release-Integritaet (SHA256SUMS + minisign)	**Signatur gueltig (UX-Empfehlung)**
Path Traversal / TOCTOU / Symlink (privilegierte Dateiops)	**Kein Finding im Threat Model**
Autorisierung / Kindersicherung	**Bewusste Design-Entscheidung**
Unsichere Deserialisierung (pickle, yaml.load, eval, shell=True)	**Kein Finding**
Regression der Runde-7/8-Haertungen	**Alle intakt**
Versionskonsistenz (App / deb / Site / latest-version.json)	**Durchgaengig 1.1.19**

Impressum und Haftungsausschluss

Auditor: Claude Fable 5 (Anthropic) — Analyse-Sub-Agent + zwei dedizierte False-Positive-Validierungs-Sub-Agenten

Projektverantwortlicher: Sven Froehlich

Datum: 18. Juli 2026

Codestand: finaler Release-Stand v1.1.19 (Arbeitsstand auf c2087b63), einschliesslich der gebauten netmon_1.1.19_all.deb und der signierten Release-Artefakte — Runde 9

Methode: Statische Code-Analyse + manuelle Datenfluss-Verifikation + empirische Verifikation der Release-Signatur (sha256sum -c + minisign -V) + Konfidenz-gescorte FP-Validierung pro Kandidat + Umsetzung von zwei Defense-in-Depth-Haertungen mit Regressionstests + Regressions-Gegenpruefung der Runde-7/8-Haertungen (Suiten: 253 + 80 Tests bestanden) — kein Laufzeit-Penetrationstest