NetMon Security Audit 2026 - Runde 12

Version: 1.1.21

Code-, Paket- und Release-Security-Review fuer NetMon Roots.

Inhaltsverzeichnis

NetMon Security Audit 2026 - Runde 12

NetMon Security Audit 2026 - Runde 12

- Kurzurteil
- Umfang
- Methodik
- Findings
  - NM-R12-01 - Paketinstallation aendert aktive DNS-Profile ohne Opt-in
  - NM-R12-02 - Firefox-TAR-Pruefung verwirft keine Links
  - NM-R12-03 - Signatur-Vertrauen startet von derselben Web-Origin
  - NM-R12-04 - Release-Versionen sind nicht aus einer Quelle abgeleitet
  - NM-R12-05 - Security Policy nennt alte Supportlinien
- Validierte False Positives
  - SHA-1-Verwendungen
  - Direkte TAR-Pfadtraversierung
  - URL-Oeffnungen
- Positive Kontrollen
- Verifikation
- Release-Betrieb
- Einordnung

NetMon Security Audit 2026 - Runde 12

Quelle: docs/SECURITY_AUDIT_2026_R12.md

NetMon Security Audit 2026 - Runde 12

Kurzurteil

Analysierter Stand: NetMon 1.1.21, Commit e3801fa8, einschliesslich der lokalen Versions- und Website-Aenderungen vom 19. September 2026.

Ergebnis: Keine kritischen oder hohen Schwachstellen im geprueften Refactoring-Delta. Das mittlere Finding, alle drei niedrigen Findings und der Informationspunkt sind umgesetzt und durch Regressionstests abgesichert. Der echte Minisign-Public-Key ist in SECURITY.md und als kanonische Datei im Repository unabhaengig von der Download-Origin gepinnt.

Schweregrad	Identifiziert	Offen nach Umsetzung
Kritisch	0	0
Hoch	0	0
Mittel	1	0
Niedrig	3	0
Information	1	0

Die seit Runde 11 vorgenommenen UI-Auslagerungen haben keine neuen Shell-, Netzwerk-, Datei- oder Privileg-Senken eingefuehrt. Die wichtigste Aussage dieser Runde ist deshalb zweigeteilt: Das Refactoring ist aus Security-Sicht sauber, hat aber mehrere bereits vorhandene Betriebs- und Lieferkettenrisiken sichtbar gemacht. Die technisch im Repository umsetzbaren Massnahmen wurden noch in Runde 12 nachgezogen.

Umfang

Geprueft wurden:

- der komplette Diff von Runde 11 (f4744552) bis e3801fa8
- 96 Commits und 21 geaenderte Produkt-, Build- und Testdateien
- 6.807 hinzugefuegte und 5.737 entfernte Zeilen
- die ausgelagerten Tab-Builder und die neue Settings-Synchronisierung
- privilegierte Installations-, DNS-, Firewall- und Security-Pfade im Ist-Stand
- Download-, Hash-, Signatur- und Site-Build-Pfade
- die bekannten Bandit-High-Heuristiken im gesamten Python-Code
- die aktuell aufloesbaren Python-Abhaengigkeiten aus requirements.txt

Nicht enthalten waren ein externer Penetrationstest, dynamisches Fuzzing, ein kompromittierter Build-Host und die Sicherheitslage aller vom Betriebssystem bereitgestellten Programme.

Methodik

1. Diff-basierte Suche nach neuen Ausfuehrungs-, Datei-, Netzwerk- und

Privileg-Senken.

1. Manuelle Datenflusspruefung der sicherheitskritischen Treffer.
2. Statische Analyse mit Ruff-Security-Regeln und Bandit 1.9.4.
3. Abhaengigkeitspruefung mit pip-audit 2.10.1.
4. Shellcheck fuer Release-, Build- und Verifikationsskripte.
5. Sicherheitsnahe Regressionstests, vollstaendige Testsuite und GUI-Smoke-Test.
6. False-Positive-Pruefung fuer jeden Bandit-High-Treffer.

Findings

NM-R12-01 - Paketinstallation aendert aktive DNS-Profile ohne Opt-in

Schweregrad: Mittel Status: Behoben am 19. September 2026 Bereich: scripts/build_netmon_deb.sh:220-306

Der generierte Debian-postinst setzt fuer alle aktiven, nicht als VPN klassifizierten NetworkManager-Verbindungen 8.8.8.8 und aktiviert ipv4.ignore-auto-dns. Anschliessend werden die Verbindungen neu aktiviert. Das geschieht waehrend der Paketinstallation ohne gesonderte Zustimmung in NetMon.

Auswirkung: In Unternehmens-, Split-DNS-, lokalen Entwicklungs- oder datenschutzsensiblen Umgebungen kann die Installation interne Namensaufloesung unterbrechen, DNS-Anfragen unbeabsichtigt an Google senden oder einen kurzen Netzwerkausfall ausloesen. Die vorherigen Werte werden zwar mit Modus 0600 gespeichert und bei der Deinstallation wiederhergestellt, das reduziert aber nicht die Auswirkung waehrend der Nutzung.

Angriffsvoraussetzung: Kein Remote-Angriffspfad. Ein Benutzer muss das Paket bereits mit Root-Rechten installieren. Die Bewertung als Mittel beruht auf Datenschutz und Verfuegbarkeit, nicht auf Codeausfuehrung.

Empfehlung: DNS-Aenderungen aus postinst entfernen. Beim ersten Start eine erklaerte, ausdrueckliche Opt-in-Aktion anbieten, die betroffene Profile, Zielresolver, Vorschau und Rollback zeigt.

Umsetzung: Der DNS-Schreibpfad und der feste Resolver wurden aus postinst entfernt. Neue Installationen veraendern keine aktiven Profile. restore_legacy_install_dns stellt beim Upgrade noch vorhandene Altzustaende wieder her und entfernt danach die alte Statusdatei. Der bestehende prerm-Rollback bleibt fuer alte Installationsablaeufe erhalten.

NM-R12-02 - Firefox-TAR-Pruefung verwirft keine Links

Schweregrad: Niedrig Status: Behoben am 19. September 2026 Bereich: netmon/app.py:32342-32406

Der Firefox-Basisinstaller prueft Archivnamen gegen direkte Pfadtraversierung, ruft danach aber tarfile.extractall() ohne Filter auf. Symbolische und harte Links werden weder verworfen noch auf ein Ziel innerhalb des temporaeren Extraktionsverzeichnisses begrenzt. copytree(..., symlinks=True) uebernimmt solche Links anschliessend bewusst in die installierte Browserbasis.

Auswirkung: Ein manipuliertes Archiv kann Links aus dem Zielbaum zeigen lassen. Nachfolgende stat-/chmod- oder Startpfade koennen diesen Links folgen. Der praktische Schweregrad ist begrenzt, weil der einzige Aufrufer eine fest hinterlegte HTTPS-Adresse von Mozilla verwendet und ein kompromittierter Download ohnehin ausfuehrbaren Browsercode liefern koennte.

Empfehlung: Nur regulaere Dateien und Verzeichnisse akzeptieren, Link- und Device-Member ablehnen und unter Python 3.12 einen restriktiven filter="data" plus eigene Zielpruefung verwenden. Downloadgroesse und entpackte Gesamtgroesse begrenzen.

Umsetzung: Eine eigene Extraktionsroutine akzeptiert ausschliesslich regulaere Dateien und Verzeichnisse, verwirft Links und Sonderdateien und validiert alle kanonischen Zielpfade vor dem ersten Schreibzugriff. Download, Memberzahl und entpackte Gesamtgroesse sind begrenzt. Dateirechte werden ohne Setuid-/Setgid-Bits uebernommen; copytree konserviert keine Links mehr.

NM-R12-03 - Signatur-Vertrauen startet von derselben Web-Origin

Schweregrad: Niedrig Status: Behoben am 19. September 2026 Bereich: site/downloads.html:151-180, scripts/verify_netmon_signature.sh:1-33

Die Schnellpruefung laedt Paket und SHA256SUMS von derselben Origin. Die Vollpruefung laedt zusaetzlich Signatur, Verifikationsskript und Public Key von derselben Origin. Bei einer kompromittierten Website kann ein Angreifer damit alle Bestandteile gemeinsam ersetzen. Minisign schuetzt in diesem Ablauf vor Transportfehlern, schafft ohne extern gepinnten Schluessel aber keinen unabhaengigen Vertrauensanker gegen eine kompromittierte Downloadseite.

Empfehlung: Public-Key-Fingerprint zusaetzlich in SECURITY.md, im GitHub-Repository und in Release Notes veroeffentlichen. Fuer produktive Releases den Build abbrechen, wenn Signatur oder Public Key fehlen. Die Schnellpruefung sichtbar als reine Integritaets-, nicht Herkunftspruefung kennzeichnen.

Umsetzung: Site- und Release-Update-Build brechen standardmaessig ab, wenn minisign, Secret Key oder Public Key fehlen. Die erzeugte Signatur wird noch im Build mit dem gelieferten Public Key verifiziert. Ein unsignierter lokaler Test-Build erfordert das ausdrueckliche Opt-out NETMON_ALLOW_UNSIGNED_BUILD=1. Der Nutzer-Verifier kann mit NETMON_EXPECTED_MINISIGN_PUBKEY eine unabhaengig bezogene Key-Zeile pinnen; die Downloadseite bezeichnet den SHA-256-Check jetzt korrekt als reine Integritaetspruefung.

Der kontrolliert erzeugte Public Key mit ID 54BF5F1867BDD004 ist wortgleich in SECURITY.md und docs/security/netmonroots.minisign.pub veroeffentlicht. Release-Builds verwenden diesen Pin standardmaessig und lehnen abweichende explizite Public Keys ab.

NM-R12-04 - Release-Versionen sind nicht aus einer Quelle abgeleitet

Schweregrad: Niedrig Status: Behoben am 19. September 2026 Bereich: netmon/config/constants.py:3, scripts/build_netmon_site_bundle.sh:5-8, site/latest-version.json:2

Zum Auditzeitpunkt standen App, Debian-Build und Manpages lokal auf 1.1.21. Site-Build, Downloadseite, Dokumentations-Build und latest-version.json standen noch auf 1.1.19; der Site-Build verwies ausserdem auf Audit Runde 11.

Auswirkung: Ein Release-Bundle kann alte Artefakte, alte Pruefbefehle und neue Changelog-Aussagen mischen. Das ist kein direkter Exploit, untergraebt aber die Zuverlaessigkeit der Integritaets- und Updatekommunikation.

Empfehlung: Eine kanonische Versionsquelle nutzen und vor jedem Build hart pruefen, dass App, Debian-Paket, Downloadseite, Update-JSON, Doku und Auditstand zusammenpassen. Solange 1.1.21 nur ein interner Entwicklungsstand ist, ist die Abweichung akzeptabel; fuer die Veroeffentlichung nicht.

Umsetzung: Debian-, Doku-, Site- und Release-Update-Build lesen die Version ueber scripts/read_netmon_version.py direkt aus netmon/config/constants.py. scripts/check_release_consistency.py prueft vor Site-Builds Update-JSON, Downloadpfade, deutsche und englische Seiten, Dokumentation und Security Policy. Alle aktuellen Releaseangaben stehen auf 1.1.21; historische Changelog- und Auditseiten bleiben unveraendert.

NM-R12-05 - Security Policy nennt alte Supportlinien

Schweregrad: Information Status: Behoben am 19. September 2026 Bereich: SECURITY.md:3-13

Zum Auditzeitpunkt nannte die Policy 1.1.17 und 1.1.16 als unterstuetzt, obwohl der lokale Stand 1.1.21 war und die oeffentliche Downloadseite 1.1.19 anbot. Dadurch blieb fuer Melder und Benutzer unklar, welche Linie Sicherheitsfixes erhaelt.

Empfehlung: Beim Release die Supportmatrix aktualisieren und zwischen oeffentlicher Version und internem Entwicklungsstand unterscheiden.

Umsetzung: SECURITY.md nennt 1.1.21 als unterstuetzte Release-Linie, kennzeichnet aeltere Versionen als nicht unterstuetzt und grenzt interne Entwicklungsstaende ausdruecklich ab.

Validierte False Positives

SHA-1-Verwendungen

Bandit bewertet drei SHA-1-Aufrufe als High. Sie werden ausschliesslich fuer kurze, deterministische Namen verwendet: Tooltip-Schluessel, kompakte interne WireGuard-Profilnamen und projectM-Dateinamen. Es werden keine Passwoerter, Signaturen, Zertifikate oder Integritaetswerte damit geschuetzt. Ergebnis: kein Security-Finding. Alle drei Aufrufe tragen nach der Nachhaertung usedforsecurity=False, wodurch die Absicht fuer Werkzeuge eindeutig ist.

Direkte TAR-Pfadtraversierung

Bereits zum Auditzeitpunkt wurden Archivnamen vor der Extraktion kanonisiert und mussten im temporaeren Ziel bleiben. Klassische ../- und absolute Pfade waren damit blockiert. Die Umsetzung von NM-R12-02 ersetzt extractall() nun vollstaendig und verwirft zusaetzlich Links und Sonderdateien.

URL-Oeffnungen

Die im Delta relevanten Downloads werden aus festen Projektkonstanten gespeist. Die Refactoring-Aenderungen haben keine neue Benutzereingabe an urlopen() angebunden. Ergebnis: kein neuer SSRF- oder lokaler Dateizugriffspfad.

Positive Kontrollen

- Keine Nutzung von shell=True, eval() oder unsicherem pickle im

gepruefteten Delta.

- Privilegierte Aktionen verwenden weiterhin argv-Listen und bestehende

sudo -n-/Bestaetigungsablaeufe.

- Die ausgelagerten Security-Tabs binden bestehende Controller-Callbacks und

fuehren keine neuen Systembefehle aus.

- ClamAV-, RKHunter-, Firewall-, VPN- und Baseline-Regressionstests sind gruen.
- Bandit meldet in den neu ausgelagerten Modulen 0 mittlere und 0 hohe Punkte.
- pip-audit meldet fuer die aktuell aufgeloesten Anforderungen keine bekannten

Schwachstellen.

- Shellcheck meldet fuer die gepruefteten Release- und Verifikationsskripte keine

Fehler.

Verifikation

Pruefung	Ergebnis
Ruff auf dem Refactoring-Delta	bestanden
Ruff S202/S324 nach Umsetzung	keine Treffer
Bandit 1.9.4, gesamtes netmon/, High-Schwelle	keine Treffer
Bandit, neu ausgelagerte Module	0 High, 0 Medium, 31 Low-UI-Ausnahmen
pip-audit 2.10.1	keine bekannten Schwachstellen
Shellcheck	bestanden
Sicherheitsnahe Tests	651 bestanden, 1 uebersprungen
R12-Sanierungsregressionen	33 bestanden
Vollstaendige Testsuite nach Umsetzung	2595 bestanden, 2 uebersprungen
Black-Check	bestanden
GUI-Smoke-Test mit Xvfb	bestanden

Release-Betrieb

Alle in Runde 12 identifizierten Massnahmen sind im Repository umgesetzt. Der passphrasegeschuetzte Secret Key bleibt ausschliesslich ausserhalb des Repositories. Der finale Produktions-Build muss deshalb bewusst durch den Release-Verantwortlichen in einem interaktiven Terminal signiert werden; ohne erfolgreiche Signatur bricht der Build ab.

Einordnung

Runde 12 ist eine statische Code- und Release-Prozesspruefung. Sie ersetzt keinen unabhaengigen Penetrationstest und garantiert keine vollstaendige Fehlerfreiheit. Die Ergebnisse gelten fuer den oben genannten lokalen Codestand und muessen nach sicherheitsrelevanten Aenderungen neu bewertet werden.