Security assessments for software that matters.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Cure53 Security Assessment of Surfshark VPN Architecture & Crypto, Management Summary, 03.2026

Cure53, Dr.-Ing. M. Heiderich, Dr. D. Bleichenbacher, Dr. S. Mazaheri, MSc. A. Schloegl, MSc. C. Mayr

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test and source code audit on the Surfshark VPN Dausos protocol, with a specific focus on the connected architecture and cryptography.

The engagement, requested in January 2026 by Surfshark, sought to verify the security proficiency of the aforementioned features. The investigation phase took place during CW09 in February and March 2026. Cure53 utilized an allocation of sixteen person-days for extensive research to ensure the depth and quality of the findings within this one-week window.

The scope tasks were grouped into five unique Work Packages (WPs), outlining the core aspects due for inspection:

- **WP1**: White-box pen.-tests & code audits against VPN architecture & threat model
- **WP2**: White-box pen.-tests & code audits against VPN control channel & state handling
- **WP3**: White-box pen.-tests & code audits against VPN data channel & packet handling
- **WP4**: White-box pen.-tests & code audits against crypto design & key exchange
- **WP5**: White-box pen.-tests & code audits against session mgmt, rekeying & PFS

Cure53 has conducted multiple previous audits of the Surfshark VPN, with the most recent engagement concluded in July 2025 (refer to report NOR-24). Notably, this current assessment represents the first instance in which the scope has focused primarily on architecture and cryptography of the Dausos protocol.

The project was conducted by four senior consultants from Cure53, who managed the entire lifecycle from initial preparation to the final delivery of documentation. Following a white-box methodology, the team utilized provided source files and relevant technical materials to perform the analysis. To ensure that technical efforts could begin without disruption, all preparatory work was finalized in CW08 (February 2026). This allowed the project to proceed in a seamless manner from the outset.

To ensure a transparent and collaborative engagement, Surfshark and Cure53 utilized a private, dedicated Slack channel for all communications. This space was open to all participating personnel from both organizations throughout the project. The project proceeded without setbacks or blockers at any stage. Productive interactions and a thoroughly constructed scope ensured that objectives were clear from the beginning, resulting in a minimal need for clarifying queries.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

For High severity findings, a limited live-reporting process was implemented, utilizing the dedicated Slack channel for immediate information sharing. Cure53 further supported project transparency by offering periodic status updates on interesting observations and overall progress.

Following thorough coverage of all work packages, the assessment resulted in ten documented findings. Of these, seven were classified as security vulnerabilities and three as miscellaneous issues or best-practice recommendations. It is important to highlight that the most severe vulnerabilities identified during the audit were localized to the external hosting environment rather than the Surfshark VPN Dausos protocol or its source code. Consequently, these were categorized as out-of-scope (OOS) for the core protocol assessment. The remaining eight findings, all of which were situated within the Dausos protocol's scope, were rated at Medium severity or lower.

With no findings rated at Critical or High severity within the actual Dausos protocol itself, the audit results reflect a stable and resilient platform. The Surfshark team demonstrated a significant commitment to security by remediating the majority of the findings immediately following the testing phase. These resolutions were subsequently presented to Cure53 for formal verification.

To ensure long-term resilience, it is essential for Surfshark to develop a formal protocol specification and a comprehensive threat model. These documents will help enumerate latent risks and balance security requirements with performance optimization. Due to the complexity of the proposed strategies, Cure53 recommends a dedicated follow-up assessment.

To highlight the PQS capabilities of the Surfshark VPN Dausos protocol, it is noted that the protocol offers post-quantum security by means of post-quantum key encapsulation and signature schemes. More precisely it implements a hybrid key-exchange protocol combining a key established through ephemeral ML-KEM and a key established through ECDH to obtain a hybrid shared key. This key-exchange is performed inside a hybrid TLS 1.3, where the server in addition to a classic RSA-certificate as part of TLS authentication, provides a ML-DSA signature (and the corresponding certificate) on a challenge chosen by the client to guarantee post-quantum authentication. Incorporating ML-DSA was done as part of a post-audit fix. The 256-bit shared key is subsequently used with AEGIS-encryption in the VPN data channel to encrypt the client-server communication.

Cure53 would like to thank Karolis Kačiulis, Tomas Stamulis, and Nikodemas Žaliauskas from the Surfshark team for their excellent project coordination, support, and assistance, both before and during this assignment.