Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Cure53 Security Assessment of Surfshark Management Summary, 04.2021

Cure53, Dr.-Ing. M. Heiderich, J. Larsson

Cure53, which is a Berlin-based IT security consultancy, completed a security assessment of the Surfshark complex in 2021. The core aim of the project was to thoroughly examine and evaluate the security posture exposed by the Surfshark server, VPN configuration, as well as the related infrastructure. To be able to issue a reliable verdict about the components in scope, the Cure53 team carried out a configuration audit and a broader security assessment. In addition, in the final phase of the project, the testing team verified fixes that the Surfshark team crafted in response to the identified flaws, as well as selected recommendations proposed by Cure53.

In terms of resources, methods and timeline, it should be clarified that two members of the Cure53 team were tasked with this project, based on their skills and expertise matching the examination's goals. They spent seven person-days on the scope, investing time into testing during Calendar Weeks 11 and 12, which corresponds to the second half of March 2021. It has been agreed that a so-called white-box methodology fitted best with the objectives that the Surfshark Ltd. entities set for this engagement. Subsequently, Cure53 was given access to five Surfshark VPN servers.

In order to optimally structure the work against the objectives communicated by Surfshark, Cure53 completed the tasks under two, specifically delineated work packages (WPs). In WP1, reviews and audits centered on the Surfshark server configuration, whereas WP2 shifted the focus to the Surfshark VPN configuration, again leveraging the same general approaches of reviews and audits.

The test started on time and moved forward at a speedy pace, thanks in part to all preparations comprehensively completed by Surfshark in CW10. The relevant members of the Surfshark and Cure53 teams were connected through a dedicated, shared Slack channel. Not many discussions were needed in light of the scope's general clarity. Still, Cure53 issued regular status updates, therefore making it possible for the Surfshark team to consult on the optimal mitigation strategies.

The coverage reached in this test was very good. Four security-relevant discoveries have been made and all resided in the realm of general weaknesses with relatively manageable exploitation potential. The highest levels of severity ascribed to problems in the project stood at

Dr.-Ing. Mario Heiderich, Cure53
Bielefelder Str. 14
D 10709 Berlin
cure53.de · mario@cure53.de

Medium. Such scores concerned two findings which might give an attacker who has already gained an initial foothold into the architecture a bit more control over the internal network. All other findings were of lower severity levels, which should be interpreted as a good sign for the security and privacy properties of the Surfshark server and VPN configuration.

Standing out among the very few concerns was the outdated *sudo* version that had not been patched. Cure53 pointed out the importance of constantly monitoring the security updates for all servers and features. A more comprehensive handling of this realm can ensure that software recognized as prone to bugs cannot weaken the overall posture of the complex. In addition, Cure53 observed that accounting for the possibility of a local attacker should be the aim taken on by Surfshark. More specifically, in regard to further development of the infrastructure, it is advised to invest time into developing a topology based on the concept of assumed-breach instead of adhering to the current security model that is established on the definition of an inside and outside security boundaries. After the submission of the report, all issues have been tackled by the Surfshark team in the weeks following the project. Cure53 verified two items as fixed, whereas the other two issues were reviewed more generally and considered appropriately handled as well.

In Cure53's expert opinion, this project confirmed a very solid security premise at Surfshark. The overall outcome should be regarded as good and the testing team has no doubt that the Surfshark maintainers have a clear understanding of security and privacy challenges associated with being a VPN provider. The VPN protocols and their attached configuration implemented by Surfshark rely on sound defaults and are additionally fine-tuned by attention to detail in configuration of constructs, logging and cipher-suites. Absence of server-side configuration that relies on insecure defaults, together with averting common misconfiguration issues, indicate great good maturity level of the Surfshark complex. Despite extensive searches and exemplary coverage toward a plethora of possible risks, no serious issues were detected.