Fine penetration tests for fine websites

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

Pentest-Report Surfshark VPN Extension 11.2018

Cure53, Dr.-Ing. M. Heiderich, BSc. T.-C. “Filedescriptor” Hong

Index

Introduction
Scope
Identified Vulnerabilities
SRF-01-002 OOS: Invitation mail uses unencrypted HTTP link (Low)
Miscellaneous Issues
SRF-01-001 Extension: Unused insecure HTTP protocol in proxy config (Info)
Conclusions

Introduction

> *“Surfshark is ahead of the curve in technological advancement, but your experience is the number one priority. Our VPN will ensure online privacy for your whole family - simple and intuitive on the outside with a robust security mechanism inside. Enjoy the full richness of the borderless internet, freely and safely on all your devices.”*
>
> From https://surfshark.com/

This report documents the results of a security assessment targeting the Surfshark VPN browser extensions. Carried out by Cure53 in November 2018, this project yielded only two security-relevant findings with limited severities and impact.

It should be noted that the assessment comprised both a penetration test and a code audit. The aim of the project was to gain an external view as to how well the Surfshark VPN browser extensions in scope handle security and privacy. In particular, it was verified whether promises made to the users about the protections against IP leaks and DNS leaks are kept. Besides the general, so-called classic browser extensions audit, the use of PAC script and fixed server settings were also placed in scope. In addition, Squid servers were checked to ensure no internal endpoints could be accessed. All in all, Cure53 relied on a so-called white-box methodology.

In order to fulfill the objective delineated above, Cure53 was tasked with investigating Chrome and Firefox extensions related to the project. Relevant source code was provided to the testing team to enable full coverage. In terms of specific resources, the

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

tasks linked to tests and audit were conducted by two members of the Cure53 who worked against a time budget of five days.

The project moved forward in accordance with the timeline and the Cure53 team executed the assessment in early November 2018. Guest accounts on a dedicated Slack channel were furnished to Cure53 by Surfshark to maintain communications with the Cure53 team during the test. As already noted, the assessment only unveiled two security-relevant issues. Further, only one was deemed to be an actual vulnerability with "*Low*" impact and the second flaw was considered a general weakness. Foreshadowing the conclusions, this is clearly a good result.

In the following sections, the report will first briefly comment on the scope and then discusses both findings on a case-by-case manner, furnishing both technical backdrops and relevant advice on mitigation strategies going forward. In light of the findings, Cure53 issues a broader verdict on the state of security found on the Surfshark VPN extensions in the final section of this report.

Scope

- **Surfskark VPN Browser Extensions**
  - https://chrome.google.com/webstore/detail/surfshark-vpn-proxy/ailoabdmgclmfmhdagmlohpjlbpffblp
  - https://addons.mozilla.org/en-US/firefox/addon/surfshark-vpn-proxy/
  - Sources were made available to Cure53
  - Test user-accounts were made available to Cure53

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

Identified Vulnerabilities

The following sections list both vulnerabilities and implementation issues spotted during the testing period. Note that findings are listed in a chronological order rather than by their degree of severity and impact. The aforementioned severity rank is simply given in brackets following the title heading for each vulnerability. Each vulnerability is additionally given a unique identifier (e.g. *SRF-01-001*) for the purpose of facilitating any future follow-up correspondence.

SRF-01-002 OOS: *Invitation* mail uses unencrypted HTTP link *(Low)*

It was found that the links embedded in the *invitation* emails rely on an unencrypted HTTP channel. An attacker who has the ability to eavesdrop (i.e. a Man-in-the-Middle adversary) on the connection of a user can take advantage of techniques like *sslstrip*[1] to proxy clear-text traffic to the victim-user.

Sample Email:

```
Hello,

Welcome to Surfshark! You're just a step away from being in control of
your internet privacy and freedom.

To start using Surfshark, get our lightweight apps for Windows, Android
& iOS, or browser extensions for Chrome & Firefox.

Download now
<http://url1242.surfshark.com/wf/click?upn=bj-2BFV32dZi1QPi7w28pg-
2F4gFCdGwMbHuvy5Q6ew-
2FebWZve6qdJs7y4NiUNFoQP1X_XAJCJLcRCebflTWCtBaYALZBe5wbjdX5QQzyU6wm7pl0ryzwVqEhE
D25RHwJYpAa75CyAC42azVrAv5euCA1jYo0bYADAoNXOQ-
2BMnESdHD5VnoK00u1ta90FtSdVIneT1vzkzBLQueHRsL-2BYPQM-
2F79MSNVt7sMmUVJfdEbMYZckWb5tcYqUhCRf6KkLRte5sVW-2FLPKVhQt-2FswnXSRopqCA-3D-3D>

Enjoy your online safety,
Surfshark
```

It is recommended to embed the links with a consistent use of HTTPS.

[1] https://moxie.org/software/sslstrip/

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

Miscellaneous Issues

This section covers those noteworthy findings that did not lead to an exploit but might aid an attacker in achieving their malicious goals in the future. Most of these results are vulnerable code snippets that did not provide an easy way to be called. Conclusively, while a vulnerability is present, an exploit might not always be possible.

SRF-01-001 Extension: Unused insecure HTTP protocol in proxy config *(Info)*

It was found that the extension code has a line that configures the proxy to use an unencrypted HTTP connection. Upon further investigation, it was determined that this condition will not be met.

Affected Files:
/src/main/proxy/chrome.js
/src/main/proxy/firefox.js

Affected Code:

```
singleProxy: {
  host,
  port,
  scheme: port === 80 ? 'http' : 'https',
}
```

Even though the issue is not exploitable, it is recommended to remove the supplied line from the code. After discussing the issue with the in-house team maintaining Surfshark, it was concluded that the line would be left out despite initial development. The flaw was promptly eliminated afterwards.

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

Conclusions

As the extremely low number of findings and their limited implications clearly indicate, the results of this Cure53 assessment of the Surfshark VPN extensions position the product in a very good light. Two members of the Cure53 team, who examined the scope in November 2018, can only conclude that the tested applications make a very robust impression and are not exposed to any issues, neither in the privacy nor in the more general security realms.

All in all, the test yielded two issues, of which only one is an actual vulnerability and not even related to the browser extension itself, and the other one a general weakness. Among the findings, one seemingly out-of-scope issue was rated with *"Low"* severity and allows MitM-capable attacker to intercept traffic of the users opening an *invitation* email pointing to the Surfshark download page (see SRF-01-002). The other issue, noted under SRF-01-001, suggests a general weakness which could potentially allow connections to a unencrypted HTTP proxy server.

The findings stand out with relation to being very rare for the VPN browser extension products[2], which commonly suffer from various issues. Strengthening reliability of the results, it can be added that Cure53 employed white-box method during this assessment and reached a good level of coverage. Despite this premise and extensive efforts, the Surfshark VPN extensions held up to the scrutiny of the Cure53 testers. To sum up, Cure53 is highly satisfied to see such a strong security posture on the Surfshark VPN extensions, especially given the common vulnerability of similar products to privacy issues.

Cure53 would like to thank the entire Surfshark team for their excellent project coordination, support and assistance, both before and during this assignment.

[2] https://blog.innerht.ml/vpn-extensions-are-not-for-privacy/