Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

TunnelBear Security Assessment Summary 07.2017

Cure53, Dr.-Ing. Mario Heiderich & Team

Introduction

This technical summary report describes the results of a series of two major VPN & application and server security audits performed by the Cure53 team between November 2016 and June 2017 as requested by TunnelBear.

TunnelBear offers commercial access to VPN servers for a broad range of users and promises maximum privacy, a promise that also requires a high level of security on the side of the VPN provider themselves. For this reason, TunnelBear reached out to Cure53 in 2016, asking for a thorough VPN penetration test, source code audit, configuration review and general consulting and advice.

It needs to be noted, that the contemporary landscape of VPN providers can be characterized as highly proliferative and saturated, while also being highly unregulated. The lack of standardization, transparency and auditing allows for both the emergent and the more established competitors to issue far-reaching security & privacy promises. These promises make selecting the right provider a difficult area to navigate for regular users as well as IT professionals.

TunnelBear aimed to take these promises as serious as can be and engaged with an external testing team, Cure53. This in itself marked an uncommon move within the broader community of the arguably somewhat security-unbothered VPN providers.

Test Summary & Methodology

Expanding on the nature of the assignment summarized in this report, it must be underscored that assessments that all at once tackle the entire VPN infrastructure together with servers, clients, browser extensions, website and more, are in fact very few and far between. In that sense, the Cure53-TunnelBear project constituted a stepping stone towards investing in transparency and, ultimately, assisted in the provision of verifiably higher standards of security that the TunnelBear compound has now to offer.

The time horizon of the project was established and entailed more than thirty days of testing, communications and reporting in November and December of 2016, followed by a six-months interim phase of in-house security development at TunnelBear. After half a year, the Cure53 team returned to conduct another round of the assessment, in the summer of 2017, investing eight days of testing. Both test phases relied on a so called “white-box” methodological approach, which signifies Cure53 testers being granted access to all relevant items, servers and source code. Taking the vast scope of the

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

project into account, both teams quickly understood that open and prompt communication would be required to maintain clarity, and detail, to effectively track issues and their resolutions. The TunnelBear team's outstandingly professional and helpful assistance contributed to the achievement of covering the massive amounts of available data.

The late 2016 Audit

From a security standpoint, the first stage of Cure53 testing against the TunnelBear software revealed significant security vulnerabilities and weaknesses. The most impactful critical and high findings are summarized below:

Vulnerability	Description
Critical (3)	
Browser Extension	Extension VPN could be bypassed via loose URL matching. PAC script was configured to allow establishment of a direct connection when requests to certain hosts and URLs were being made. The matching expressions were found flawed and therefore might aid an attacker who seeks to force a victim into making a request with the VPN disabled.
Browser Extension	It was found that the VPN on the browser extension could be turned off by simply visiting a TunnelBear URL. When loaded, a malicious web page could send a message to the extension and toggle the on/off state. Given a context of the VPN already being turned on, this means that visiting the link would turn it off.
macOS Client	TunnelBear Daemon allowed local root privilege escalation through the use of a malicious program installed on the host machine.
High (3)	
API	Referrer-based CSRF protection could be bypassed allowing user to be logged out of TunnelBear.com website, subscription cancelled.
API	Possible phishing via HTML injection on invite emails. The API endpoint handling invitations was vulnerable to HTML Injection allowing attacker control over the HTML tags in the email, making it feasible for an attacker to include fake links and text to fool a user into registering on a fake website.
Android	It was found that the Android application exported its LaunchVPN activity and did not protect it with permissions. A malicious app could have leveraged those weaknesses to make the

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

	TunnelBear app crash while running in the background and potentially lose connection.
Medium (13) **Low (8)** **Informational (13)** For brevity sake, the details on the medium, low and informational severity issues are not listed below.	

All discoveries were filed into the purposely created bug tracker tool for live-reporting and documentation. Fixes and fix recommendations were discussed between TunnelBear and Cure53 using the bug tracking tool.

The mid 2017 Audit

Six months later Cure53 returned to testing the TunnelBear products. However, it was quickly agreed that the testers seemed to be encountering a hugely different project by then. First of all, it was determined that the vast majority of the formerly spotted problems had been appropriately addressed prior to the 2017 audit.

Vulnerability	Description
Critical (0)	
N/A	No issues of critical severity were spotted
High (1)	
VPN Server	Files that contained sensitive information such as internal usernames and passwords were stored with overly generous permissions. However, the attacker would need to have direct access to the server in order to retrieve these files.
Medium (4) **Low (3)** **Informational (5)** For brevity sake, the details on the medium, low and informational severity issues are not listed below.	

The deployed fixes held up to verification and scrutiny, while some additional repairs and mitigation strategies were still being developed. Secondly, retesting of the TunnelBear project over the course of eight days of testing work in the summer of 2017 revealed a much lower number of only thirteen findings.

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

More importantly, no issues of critical severity were spotted, and the vulnerabilities mostly represented medium- to low-risk categories of findings. As such, they did not call for urgent fixes and the risks they exposed could be perceived as infrastructurally acceptable, as far as protecting users was concerned (aside from the one high-severity issue that was fixed the day it was reported).

All in all, the security at TunnelBear has been moved by leaps and bounds. The impression after the second audit is in no way comparable to the one gained from the first round of testing and assessments.

Conclusions

The progress made by TunnelBear over the course of half a year demonstrates how the potential of a security audit and advice in the VPN realm may be harnessed to hoist up the safeguarding strategies within the entire software compound. After undergoing the first challenging security test which ended with several critical & high severity findings, the TunnelBear team seems to have redoubled efforts on security.

The results of the second audit clearly underline that, and TunnelBear deserves recognition for implementing a better level of security, for both the servers and infrastructure, as well as the clients and browser extensions for various platforms. The audits further went full circle in underlining, ideally to other security-affine VPN providers and their user-community, that no matter which mechanisms are at play, lacking regular external auditing negatively impacts on the effectiveness of the extended protections.

At the end, wholesome and continuous approaches must be undergirded by a dynamic view, which incorporates security into the very core of the products' development. It is apparent that the TunnelBear maintainers share this vision and are in full flight on a journey towards achieving and upholding better security standards.

Cure53 provided clear recommendations for developing good and timely fixes. More importantly, Cure53 and TunnelBear established the value of embedding security resources and regular audits into the broader projects to prevent recurrence and regressions.