Fine penetration tests for fine websites

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

IVPN Privacy & No-Log Audit Report 03.2019

Cure53, Dr.-Ing. M. Heiderich, MSc. N. Krein, J. Larsson

Index

Introduction

> *“IVPN encrypts your internet activity, shielding you from hackers, ISP's and everyone else who has no business recording what you haven't chosen to share.”*
>
> From https://www.ivpn.net/

This report documents the findings of a so-called No-Log Audit against the VPN servers of IVPN, which is a product offered by Privatus Limited. The audit, which targeted the general setup and aimed at verification of security-related claims, was executed by Cure53 in March 2019.

It should be clarified that the IVPN product is basically supposed to furnish consumers with privacy-driven VPN services. Therefore, the goal of this No-Log Audit was to acquire a verdict about the technical soundness of the privacy and security premise from a third-party - here the Cure53 team. The auditing team was tasked with evaluating whether the privacy claims made in the privacy policy of the IVPN product actually hold to technical scrutiny. With more details about the claims in the *Scope* section, the main focus of this project was on the actual technical implementation.

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

The project progressed in a timely fashion under an agreement that Cure53 would issue a verdict on the basis of the collected evidence. The first scenario was that Cure53 would need to report privacy policy violations, regardless of them being accidental or flawed by design. In this instance, IVPN would have the chance to fix the problems and Cure53 would have been responsible for fix verification. The second scenario, it was understood that Cure53 might confirm that servers and infrastructure made available by IVPN are free from all kinds of privacy and policy violations. For the latter situation, Cure53 was to document the obtained results as well.

After carefully investigating the scope of the IVPN project, Cure53 testifies that neither privacy nor policy-related violations have been observed on the audited systems in the timeframe of the audit. The three members of Cure53 assigned to undertake the project, who spent seven days examining the IVPN product through a security lens, can confirm that the product has been designed with security in mind and adheres to the privacy premise set out in the IVPN policy.

To give more details, the main focus of the audit placed on a set of two major claims made by IVPN and aggregated to the following items:

- Claim 1: **IVPN performs no logging of traffic, IP addresses or DNS requests.**
- Claim 2: **IVPN does not carry out any statistical logging of customer-traffic.**

In order to verify these two claims, Cure53 conducted investigations of the IVPN systems, choosing the items from a list provided by IPVN, which matched the list available to the public on the IVPN website. The auditors had been granted SSH access and had full privileges in consulting technical data needed for reaching a realistic verdict. Additionally, over the course of the audit Cure53 and IVPN were in contact through a dedicated Slack channel set up by Cure53 for the purpose of exchanging information and discussing potentially emerging issues.

To sum up, Cure53 detected one minor glitch in terms of potential privacy violations and reported this to the IVPN team. In-house, the issue has been promptly addressed and Cure53 verified soundness of the deployed fix. Besides this slight flaw, neither additional privacy violations nor instances of non-adherence to policy have been spotted. As such, Cure53 was able to conclude this audit with a verification of the main two claims. In the following sections, this report first discusses the scope in considerable detail. Next, the auditors elaborate on the chosen methodology and coverage of this assessment. After that, the single spotted glitch is documented and and described from a technical perspective, as well as in regard to steps undertaken upon its discovery. Finally, Cure53

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

delivers a summary of the results and reiterates the verdict about the privacy offered by IVPN in light of this March 2019 No-Log Audit's findings.

Scope

- **IVPN No-Log & Privacy Audit against Servers & Infrastructure**
  - IVPN tasked Cure53 with conducting a No-Log Audit, which is essentially a verification of the privacy claims a VPN provider has published.
  - Note that the primary scope for this No-Log Audit did not encompass the entirety of systems utilized by IVPN but only included those that are involved in serving a customer's VPN session. This signifies server audits whilst no client software was reviewed in this assessment.
  - Systems that are used for CRM purposes, billing purposes and other activities also were not audited by Cure53.
  - Cure53 shared SSH keys to get access to the servers in scope for this No-Log Audit and was able to investigate those with *root* privileges.
  - Cure53 was further given VPN customer-accounts to simulate an actual VPN session managed by the IVPN servers.
  - Cure53 was also provided with an extensive list of hosts that they could be accessed using the shared SSH public keys during this investigation.

Applied Methodology

In the following paragraphs, Cure53 outlines and discusses the testing methodologies chosen to verify the claims made by IVPN prior to the audit taking place. This section is meant to offer more transparency to the reader and more broadly provides a better overview of why and how Cure53 reached the final verdict regarding the logging claims made by IVPN. The following sections are split by claims, each subsection shedding light on a given claim and the examinations performed by Cure53 to verify or falsify each statement.

Scope Details

During this privacy-centered audit executed for IVPN, Cure53 was tasked with analyzing IVPN's privacy policy. The auditors had to ensure that the claims made regarding the logging of user-identifiable data on all VPN gateways involved in serving a customer VPN session are truthfully realized. In order to gain insight into IVPN's infrastructure, as well as to be able confirm or deny the validity of the claims, Cure53 was given access to the related gateways and authentication servers. With SSH access and accounts equipped with *root* privileges, Cure53 had a clear view into each service and its configuration.

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

IVPN's privacy policy can be summarized as follows:

- IVPN does not log any data that can be used to identify an individual user of their service, meaning during a process of a user connecting, being connected or ceasing the use of the VPN.
- Minor exceptions include temporary records of user-sessions on the authentication servers which serve to prevent abuse of simultaneous connections.

Audit Limitations

It has to be underlined that the sole focus was the privacy-related audit for the connected backend systems and that potential vulnerabilities related to the server hardening were not in scope for this engagement. This also means that leaks generated on the customer/client-side, such as DNS leaks, WebRTC leaks and similar, have been explicitly excluded from the project's scope.

Claim 1: IVPN performs no logging of traffic, IP addresses or DNS requests.

The Work Package connected to the first claim mostly included the review of all configurations of the OpenVPN and Wireguard setups, with additional audits of the customized scripts that handle authentication, port forwarding and multihop connections.

The global *config* files that are used for OpenVPN make sure to redirect all output to */dev/null*. Authentication is handled with an additional VPN tunnel to authentication servers that passes a challenge. A response is sent to a RADIUS server with MySQL as the backend storage. User-data is kept to a minimum whereas the *usernames* are randomly generated. Additional *bash* scripts run for when clients connect make sure that verbosity is kept to a minimum and the data does not touch the disk at all. The OpenVPN scripts are communicating via *unix* domain sockets, thus leaving no command line traces. The state for user-connections to handle multihop connections is entirely handled via symlinks. The latter has a positive side-effect in that no actual data lands in the data segments of the *EXT4* partitions. There are some extra command line scripts to query a user's port forwarding settings via *cURL* to an additional API, the connections are consistently established securely. While the responses are temporarily stored, they only contain a minimal set of data required to perform the task and are purged instantly.

Even though it is early days for the IVPN's Wireguard implementation, Cure53 was given access to the relevant machines and reviewed the configurations. These were found

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

satisfactory as well, mostly due to the fact that they are quite generic. The states and keys are stored via an additional configuration that uses MySQL and RabbitMQ for distribution. Cure53 was not able to spot additional changes to the Wireguard setup in that contradicted the privacy claims.

IVPN also provides their own DNS servers on the VPN gateways so that customers can make use of this to prevent DNS leaks. IVPN utilizes Unbound with a relatively standard configuration and low verbosity level. However, Cure53 found that DNS responses are automatically cached, leaving a small window for potential correlation attacks. This is described in more detail in IVP-01-001. During this engagement, IVPN promptly made sure to mitigate this issue by lowering the cache sizes to 0. Besides the above, Cure53 was unable to spot any other mechanisms that help with identifying customer information.

From Cure53's perspective gained by analyzing the servers they were given access to, it is safe to say that IVPN makes sure not to log any traffic or IP addresses of its users. The minor DNS issue was promptly mitigated and in reality caused close to no actual risk for IVPN's customers.

Claim 2: IVPN does not carry out any statistical logging of customer-traffic

The work connected to this claim covered IVPN's second statement about no statistical data about the customers' connections being kept. This includes logging of timestamps or connection durations, logging of customers' bandwidth or any other sort of account activities. The only exception concerned tracking of the simultaneous connections.

While the general targets of the audit are essentially the same as with the verification of the previous claim, the focus has been shifted onto the key items mentioned in Claim 2. This means that Cure53 audited the same configurations and connected scripts of the OpenVPN and Wireguard but zoomed in on any statistical data that might get sent to other services - such as monitoring interfaces. In sum, no observation of any deliberate customer-related logging has been noted. While there are monitoring interfaces (IVPN makes use of *Zabbix*) in place, the scripts solely pull metrics from the entire VPN nodes. This also includes bandwidth data that is read from the tunnel interfaces via *vnstat*. This essentially accounts for all VPN gateways including OpenVPN and Wireguard, where the complete VPN nodes are monitored. Cure53 can confirm that the methodology of how this is implemented leaves no option for deliberately tracking individual customers.

To summarize, Cure53 strongly believes that the claim about not logging statistical data is valid.

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

Identified Privacy Problems

The following section lists the coverage and methodology for the privacy-related audit, along with any issues found during the engagement. Each issue is given a unique identifier (e.g. IVP-01-001) for the purpose of facilitating any future follow-up correspondence.

IVP-01-001 DNS: Unbound DNS responses are cached *(Low)*

As mentioned in the coverage of the privacy claims above, Cure53 noticed a small issue with the DNS servers on the VPN gateways. While the privacy claims mention "*No DNS request logging*", it was found that DNS responses are in fact cached by the DNS software itself. While this cannot be treated as an instance of DNS request logging *per se*, it would nevertheless allow for correlation attacks, depending on how large the cache already is. On the given VPN gateways, this can be confirmed via the following *shell* excerpts.

***Shell* excerpt on *Customer*:**

```
customer@customer:~$ ping dnstest.dd.h4x.tv
PING dnstest.dd.h4x.tv(localhost6.localdomain6 (::1)) 56 data bytes
```

***Shell* excerpt for VPN Gateway:**

```
[root@de2 unbound]# unbound-control dump_cache | grep h4x
dd.h4x.tv.    289    IN    NS    ns1.h4x.tv.
dnstest.dd.h4x.tv.    289    IN    AAAA    ::1
```

In the context of a VPN provider that attempts to keep logging and caching to a minimum, this can be treated as unwanted behavior. Although the actual customer's DNS request is not logged, correlating the DNS cache with the presence of a customer-connection can yield the same result. Quite clearly, this would depend on how many entries already exist within the cache.

When spotted and confirmed, this issue was discussed with the IVPN developers who promptly developed a mitigation. The solution automatically reduces the cache size of all DNS servers on the VPN gateways to 0. As such, the recommendation for improvement in this realm has been met as the Cure53's assessment was still ongoing.

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

Conclusions

This No-Log Audit, carried out by Cure53 in March 2019 for IVPN and targeting the VPN servers has concluded with positive verification of the security claims, thus pointing to good privacy-related outcomes.

In a broader context, it needs to be stated clearly that No-Log Audits are usually quite challenging due to the commonly black and white nature of the results. On the one hand, an audit of this type can be utilized to factually check whether a certain VPN provider indeed implements what they promise in their privacy policies. On the other hand, the resulting reports about the validation of privacy claims, even assuming positive confirmation, need to be enjoyed with some caveats.

First up, the external, third-party auditors - here represented by Cure53 - are granted access to a certain number of systems for the duration of the project. Usually after about a week, they can make a determination about the state of privacy matters for the audited party. However, it is paramount to take into account that the analyzed scope tends to only be a snapshot of the wider compound. In that sense, the auditors factually investigate whether the provided selection of scope items adhere to the privacy claims that are being verified. Given this aspect, the audited party - here concerning the IVPN - could hypothetically give auditors access to specially prepared systems only. While such a rogue behavior would be of course condemned, it would be nearly impossible to detect it. While Cure53 has faith in the proper handling of privacy and the absence of logging on the IVPN project, the auditors empirically only confirm that the systems that they had access to displayed no evidence of logging.

To reiterate, this report and its positive verification of the privacy claims made by IVPN should only be read with awareness of technical limitations. While a No-Log Audit never guarantees that the audited party does not perform logging of privacy-relevant user-data “elsewhere”, it must be seen as a token of transparency and belief in their product that the audited party offers to the customers. Therefore, the investigation of the specific IVPN claims in a snapshot yielded good results for a particular timeline of March 2019.

To conclude this Cure53 audit and verification of the IVPN privacy-related claims yielded very positive results. The outcomes of this March 2019 audit, paired with fluent communications as well as the general handling of every aspect discussed during the assessment, attest to the considerable dedication to privacy matters at the IVPN project. Based on the findings, it is safe to say that all of the IVPN’s privacy statements **could be verified as truthful** within the defined scope. The requirements for both general security claims to be considered appropriate were successfully well met for all VPN gateways and authentication servers that the Cure53 auditors have been given access to. The

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

small DNS issue described in IVP-01-001 does not negatively impact this conclusion. On the contrary, discussing this problem with the IVPN developers quickly resulted in a mitigation that improved the configuration in place. Such dedication to quickly find solutions for general problems that were not originally part of the audit strengthened the positive impression acquired by the auditors. It is clear that IVPN attempts to provide exactly the service it promises and the results of this audit support the soundness of the security claims despite the strict scope definitions.

Cure53 would like to thank Nick Pestell, Fedir Nepyivoda and Iain Douglas from the IVPN team for their excellent project coordination, support and assistance, both before and during this assignment.