Fine penetration tests for fine websites

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

Pentest-Report IVPN VPN, Server & Web 01.2020

Cure53, Dr.-Ing. M. Heiderich, MSc. N. Krein, MSc. D. Weißer, J. Larsson,
BSc. J. Hector, Prof. Dr. N. Kobeissi

Index

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

Introduction

“Without a VPN you connect to the internet through your internet service provider (ISP) with no encryption. Every site you visit, and the content that you view or download, can be tracked by your ISP. It's like sending confidential messages using postcards except that unlike your post office, your ISP can record and store every message with almost zero effort and cost.”

From https://www.ivpn.net/what-is-a-vpn

This report describes the results of a broadly-scoped penetration test, security audit and fix verification process for IVPN, a provider of VPN services. The project was carried out by Cure53 in late 2019 and early 2020 and revealed nine security-relevant issues on the scope, including three items marked as *High.*

To understand the background of this project, it should be noted that this is a second iteration of security-driven work that Cure53 conducts for the IVPN entities. However, unlike the first installment in March 2019, this November-December project can be seen as a classic penetration test and a security audit. The test-targets encompassed elements of the IVPN software complex, including VPN servers and infrastructure, as well as any publicly exposed endpoints like websites and similar items. A fix verification process was executed by Cure53 after the audit and finalized in January 2020, prior to authoring of this final report document.

In terms of resources, six members of the Cure53 were involved in this assessment and executed the investigation in late November and early December 2019. The time dedicated to the completion of all project tasks amounted to twenty-one person-days in total. It was agreed that the so-called white-box methodology is best-suited for the examination of the IVPN scope. Cure53 had access to relevant source code, configuration files and servers set up for the purpose of testing.

In order to address all goals of the project in a comprehensive manner, the tasks have been structured into three work packages (WPs). In WP1, Cure53 focused on the IVPN VPN service infrastructure. Next, the servers and infrastructure took center stage in WP2. Finally, WP3 rounded up the investigation by tackling the IVPN web front-end and public sites.

The project started on time and progressed efficiently. Communications between Cure53 and the IVPN team were done in a Rocket.Chat instance created specifically to enable exchanges. Members of both the IVPN team and the Cure53 team joined this space to discuss scope and resulting questions Cure53 also used this channel to deliver status updates and furnish details about certain findings and live-reports. Some of the live-

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

reported findings were addressed by the IVPN team right away and Cure53 was able to verify the fixes while the test was still ongoing. With an effective communication strategy in place, the Cure53 team managed to obtain a very good coverage in the time available for this assessment.

As noted above, nine discoveries were made by Cure53 during this test installment. Four items belong to the category of security vulnerabilities, while the remaining five should be seen as general weaknesses, usually carrying lower exploitation potential. It should be emphasized that not only was one issue given a *Critical* severity score (which was later adjusted to be of *High* severity instead), but further two problems received a ranking of *High.* The most pressing matter stemmed from WP3 and related to the fact that the IVPN web application had no functional CSRF protection in place. More specifically, once the issue had been life-reported, it was revealed that general CSRF protection could be noted. However, as Cure53 has learnt, it had been *disabled* to help debugging an issue in the past. At that point, likely due to an oversight, it was never turned back on. This points towards room for improvement in the realm of operational security, with the matter seen as quite concerning from the Cure53's perspective.

Other weaknesses spotted in the frame of this project were also predominantly located in the realm of WP3, meaning web applications. Comparatively, the scope enveloped by WP1 and WP2 made much better impression. Only three general weaknesses were ultimately documented in connection to the first two work packages. In the following sections, the report will first present the areas featured in the test's scope in more detail, reiterating the WPs. The report closes with a conclusion in which Cure53 summarizes this November-December 2019 project and issues a verdict about the security premise of the investigated IVPN web estate, together with the VPN configuration and server setup, as well as server infrastructure.

The report's Appendix #1 and Appendix #2 will chronologically list Cure53's tickets and present the discoveries one-by-one.

Scope

- **IVPN Servers, Infrastructure & Websites**
  - **WP1**: IVPN VPN Service Infrastructure (Pentest / Configuration Review)
  - **WP2**: IVPN Server & Infrastructure (Pentest / Configuration Review)
  - **WP3**: IVPN Web Front End & Public Sites (White-Box Web Penetration Test)
- A detailed scope document was shared with Cure53
- All necessary sources were shared with Cure53
- Additional material such as OpenVPN configuration and the like were shared with Cure53

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

Audit Results

This Cure53 assessment of the IVPN entities generally concludes on a positive note, although the involved six members of the testing team managed to identify several areas that could benefit from improvements in the realm of security. After spending twenty-one days on the scope in November and December 2019, it has been concluded that findings have been spotted across all three Work Packages, though test-targets of WP3 suffered from more prominent and severe shortcomings. The presence of nine issues on the IVPN scope cannot be taken lightly and it is hoped that this late 2019 project will positively contribute to the amelioration of the overall security posture at the IVPN complex. The early 2020 fix verification process confirms that impression.

To give some details, throughout this second iteration entailing white-box testing, Cure53 had the chance to analyze the IVPN's network infrastructure. The testing period allowed for an inspection of the server setup and their hardening features, as well as offers conclusions from the general VPN config reviews. In terms of general VPN configurations, the reviewed client-to-server and server-to-server tunnel constructs rely on cipher-suites that make use of sound cryptographic algorithms. The OpenVPN configurations were deemed to be sufficiently hardened as well. Additionally, they offer good privacy and integrity for the running services.

Multihop and session management are handled in a proper and efficient way. The underlying VPN topology should be regarded as well-designed and correctly maintained. In sum, the OpenVPN configuration used by IVPN leaves a good impression, at least on the given staging environment.

The IVPN project adopts sound and privacy aware methods ensuring the originating client session is protected throughout IVPN's infrastructure. However, in order to further improve on security observable on the running infrastructure, it is recommended to run the host without physical hard drives and solely rely on volatile and encrypted RAM-drives. This would ensure that no data would be breached if the physical server were to be attacked.

Regarding general server hardening, Cure53 was able to file a couple of more or less minor recommendations, most of which are described in IVP-02-001. However IVP-02-008 is a little more alarming, since a compromised staging environment might abuse this issue to take over the remaining network. Next, the IVPN's customer-facing websites exposed additional issues. The most concerning one is a CSRF vulnerability on the main website, initially rated as *Critical*. The stated reason for the existence of this issue was a deployment of a workaround for another, related bug. Still, had this not been found, the main website of IVPN could have remained vulnerable to account-takeover for a while.

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

The examined backend services which run on top of a 3rd party CRM system were found to be satisfactory, although a few highly dangerous plugins were left in active state. These were removed during the testing period, yet the closed source policy employed by the chosen CRM system remains worrisome, particularly as it makes software auditing very hard. It is recommended to find an alternative backend management system that has a better track record and is more transparent.

To summarize, the Cure53 team leans towards a positive verdict, which should be read with the caveat that numerous items have been filled and some had significant severities. While the core product, as in the VPN construct and its network, are certainly well-designed and correctly implemented, the main concerns voiced by Cure53 relate to secondary services, which are often suboptimal and call for more attention. Despite the *High*-scored problems, Cure53 is impressed with the level and quality of engagement that the IVPN team displayed when remediating the reported findings. Just like all communications, the ensuing repairs were quick and comprehensive, attesting to the high in-house capacity within the IVPN security premises. Even with the aforementioned issues and reservations, Cure53 remains positive about the security posture at IVPN being continuously improved moving forward.

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

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

Appendix #1: Identified Vulnerabilities

The following sections list both vulnerabilities and implementation issues spotted during the testing period. Note that findings are listed in 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. *IVP-02-001*) for the purpose of facilitating any future follow-up correspondence.

IVP-02-005 WP3: Account-takeover due to missing CSRF protection *(High)*

Note that this issue was originally rated to be of Critical severity. A longer discussion with the IVPN team however resulted in Cure53 lowering the severity. The reasoning for this decision was based on the real-life impact of this finding as evaluated by IVPN

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-006 WP3: Various vulnerabilities in CRM system modules *(High)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-008 WP1/2: Use of SSH-agent can lead to full network takeover *(High)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-009 Crypto: RADIUS authentication mandates weak hashing *(Low)*

Fix Notes: *Patches ivpn.net-v2-3e5d6cd45a3b90ad66d7cd7eb127ddfc8a4ddec7 and go-services-2a235625e818b85860ac848e039a8b4aff02c06e were verified to implement above mitigations. They serve to lessen the impact of weak RADIUS password hashing and improve privacy of user-password information.*

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

Appendix #2: 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.

IVP-02-001 WP1/2: General server hardening weaknesses *(Medium)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-002 WP1/2: No Sensitive Data-Types in *puppet* configuration *(Low)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-003 WP1/2: *Swap space* can lead to unintentional logging *(Info)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-004 WP3: Split-API Injection on *admin* server *(Low)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*

IVP-02-007 WP1/2: *Bitbucket* private keys stored on server *(Medium)*

Fix Notes: *This issue was addressed by IVPN and the deployed fix was verified by Cure53.*