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 Opera VPN Server & Clients, Management Summary 03.2022

Cure53, Dr.-Ing. M. Heiderich, MSc. N. Krein, MSc. D. Weißer, MSc. F. Fäßler,
MSc. R. Peraglie, BSc. J. Hector, Dr. A. Pirker

Cure53, which is a Berlin-based IT security consultancy, completed a security assessment of the Opera VPN clients, servers and periphery, developed by Opera Norway AS. The core aim of this September 2021 project was to thoroughly examine and evaluate the security posture exposed by the Opera VPN software, alongside client software, server-side implementations and several peripheral elements such as the Opera Mini-protocol for VPN Config delivery.

To be able to issue a reliable verdict about the components in scope, the Cure53 team carried out a series of penetration tests, code audits and security examinations. In addition, in the final phase of the project, the testing team verified fixes that the Opera team crafted in response to the identified shortcomings and recommendations proposed by Cure53.

In terms of resources, methods and timeline, it should be clarified that seven members of the Cure53 team were tasked with this project. The senior testers were chosen on the basis of their skills and expertise matching the examination's goals. The Cure53 team spent twenty-four person-days on the scope, investing time into testing during mid September 2021 (CW36, CW37). It should be underlined that Cure53 was given access to all relevant source code that fuels the software compound. The white-box premise of this assessment was clearly motivated by the intention to maximize the depth and breadth of the coverage.

In order to make sure that all aspects of the scope receive proper attention, the work was split into four Work Packages (WPs):

- **WP1**: White-Box Tests against Opera VPN Client-Side Implementations
- **WP2**: White-Box Tests against Opera VPN Server configuration & Infrastructure
- **WP3**: High-level Review of Opera Mini-protocol for VPN Config delivery
- **WP4**: High-level Review of Opera VPN Software Security Processes

The test started on time and moved forward at a speedy pace, thanks in part to all preparations comprehensively completed by Opera in CW35. The relevant members of the Opera VPN project team and the Cure53 testers were connected through a shared and dedicated Slack channel, which merged the workspaces of the two partaking entities.

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

Pertinent test-supporting information and a thorough walk-through proffered by the Opera team assisted the tests immeasurably. Furthermore, Cure53 issued regular status updates and live-reports, therefore making it possible for the Opera team to consult on the optimal mitigation strategies.

Efficient progress with the assessment translated to reaching a very good coverage of the WP1-WP4 test-targets. A total of fourteen security-relevant issues have been spotted and documented, indicating a rather mixed result of this investigation for the team behind the Opera VPN software complex. Eight issues represented actual vulnerabilities and the remaining six resided in the realm of general weaknesses with limited exploitation potential. Five findings constituted a high severity rating but luckily, none were given critical severity ratings. All findings have been live-reported to the Opera team and were addressed over the course of the following weeks.

Finding ID	Work Package	Status	Comment
OPR-01-001	**WP3** (Mini)	**Partly fixed**	
OPR-01-002	**WP2** (VPN)	**Fixed**	The fix was verified by Cure53
OPR-01-003	**WP3** (Mini)	**Risk accepted**	Non-issue in VPN context
OPR-01-004	**WP3** (Mini)	**Risk accepted**	Non-issue in VPN context
OPR-01-005	**WP3** (Mini)	**Risk accepted**	
OPR-01-006	**WP1** (VPN)	**False alert**	
OPR-01-007	**WP2** (VPN)	**Fixed**	The fix was verified by Cure53
OPR-01-008	**WP3** (Mini)	**Fixed**	The fix was verified by Cure53
OPR-01-009	**WP3** (Mini)	**WIP**	
OPR-01-010	**WP2** (VPN)	**Fixed**	The fix was verified by Cure53
OPR-01-011	**WP2** (VPN)	**Fixed**	The fix was verified by Cure53
OPR-01-012	**WP2** (VPN)	**Fixed**	The fix was verified by Cure53
OPR-01-013	**WP2** (VPN)	**Fixed**	The fix was verified by Cure53
OPR-01-014	**WP3** (Mini)	**Fixed**	The fix was verified by Cure53

Table.: Fix status as of March 2022

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

As noted, most of the relevant vulnerabilities have now been tackled by Opera and were verified as fixed by Cure53 in the weeks following the project.

More precisely, eight of the spotted items were analyzed by Cure53 in relation to diffs and confirmed as mitigated properly, one issue was partly fixed and the fixes were reviewed. Of the remaining five flaws, three were flagged as acceptable risks because the factors around them are tightly controlled, one was flagged a false alert and one is still a work in progress.

In conclusion, drawing on the evidence gathered during testing and subsequent fix verification, one can clearly argue that the outcomes highlight the Opera VPN development team's commitment to maintaining security features with due diligence and adherence to best practices.

This Cure53 project shows that the overall security strength of the Opera VPN clients, servers and periphery software including its periphery delivers, after fix verification having concluded, good impressions, particularly with regard to injection attacks, malicious users and external data access from sources outside of the organization as no injection-related or access-control issues were left unfixed.

The Opera VPN software compound is, in Cure53's opinion, currently well-protected against a broad number of mobile-application- desktop-, network- and server-security related attack vectors, as corroborated by the number and quality of the submitted fixes and the subsequent successful fix verification.