Fine penetration tests for fine websites

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

Security Assessment of RealVNC Software & Clients Management Summary, 01.2022 - 05.2022

Cure53, Dr.-Ing. M. Heiderich, N. Hippert, BSc. J. Hector, MSc. D. Weißer, BSc. C. Kean, MSc. R. Peraglie, MSc. J. Moritz, Dr. A. Pirker, Dipl.-Inf. G. Kopf, Dipl. Inf. M. Münch

> *"To conclude, this early 2022 assessment combined with the April & May 2022 fix verification confirm that the RealVNC Connect Remote Access service in scope is now perceivable as strong and stable regarding security posture"*

Cure53, which is a Berlin-based IT security consultancy, completed a clearly scoped and targeted security assessment of all components of the VNC Connect Remote Access service - namely the VNC Server; the VNC Viewer Desktop & Mobile; the Direct & Cloud Connections; the Connect Portal; the Connect Authentication Service; the VNC Connect Directory Service; and Hosted Services.

The work was requested by RealVNC Limited in October 2021 and got carried out by Cure53 from mid-January to early-March 2022, namely between CW03 and CW09.

As for the precise timeline and specific resources, Cure53 completed the examination parts in CW10 of 2022 by handing over a detailed penetration test report (VNC-01). A grand total of eighty-six person-days were invested to reach the coverage expected for this large-scale assignment, whereas a team of ten testers has been composed and tasked with this project's preparation, execution and finalization. The project progressed effectively on the whole. All preparations were done in CW07 and CW08, so as to foster a smooth transition into the testing phase.

Namely, to allow better tracking and equilibrium in terms of testing, the scope was split into four work packages (WPs) corresponding to the distinct areas described below:

- **WP1**: White-box penetration-tests against RealVNC VNC server and VNC Viewer desktop & mobile, direct and cloud connections
- **WP2**: White-box penetration-tests against RealVNC VNC Connect Portal
- **WP3**: White-box penetration-tests against RealVNC VNC Connect Authentication Service and VNC Connect Directory Service
- **WP4**: White-box penetration-tests against RealVNC Hosted Services

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

It can be derived from the above that white-box methodology was utilized for all WPs to achieve the expected coverage- and depth-levels.

Cure53 was given access to URLs, binaries, in-scope applications and APIs, application source codes, alongside test-users and further test-supporting material. Additionally, API documentation was provided to make sure the project can be executed in line with the agreed-upon framework.

Communications were facilitated via a dedicated, private Microsoft Teams channel deployed to combine the workspaces of RealVNC and Cure53, thereby allowing an optimal collaborative working environment to flourish. All participatory personnel from both parties were invited to partake throughout the test preparations and discussions. One can denote that communications proceeded smoothly on the whole. The scope was well-prepared and clear, no noteworthy roadblocks were encountered throughout testing, and cross-team queries were kept to a minimum as a result. RealVNC delivered excellent test preparation and assisted the Cure53 team in every respect to procure maximum coverage and depth levels for this exercise.

The Cure53 team managed to get very good coverage over the WP1-4 scope items. Among thirty-eight security-relevant discoveries, thirteen were classified to be security vulnerabilities and twenty-five to be general weaknesses with lower exploitation potential. The extensively vast scope and ample testing days assigned for this audit fostered the expectation that a fairly numerous volume of findings would be unearthed. Even so, the detection of thirty-eight findings should not be considered a cause for concern due to the relatively moderate severity of the issues grouped as a whole.

In fact, no issue was granted a *Critical* severity rating and only three were deemed *High*. This evidently implies that the RealVNC team places a strong focus on the security posture of all components in scope, though nevertheless demonstrates that leeway for targeted improvements certainly persists in order to elevate security to an exemplary level.

As a final stage of this project in late April and early May 2022, Cure53 engaged in and completed a phase of fix verification, inspecting how the RealVNC scope has improved over time and in relation to the communicated findings. In this realm, the testing team is happy to report that thirty-two of the reported vulnerabilities and miscellaneous issues have been properly addressed, with recommendations stemming from the assessment followed correctly. Only six issues were flagged as either false-alerts or works-as-intended and all of them were initially evaluated to be of lower risk.

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

Cure53 was able to inspect the fixes by getting access to commits & pull requests and means to review those. This was done in orchestration with two of the involved Cure53 team-leads who were given access to the code changes via remote VM access.

To conclude, this early 2022 assessment combined with the April & May 2022 fix verification confirm that the RealVNC Connect Remote Access service in scope is now perceivable as strong and stable regarding security posture.

From the Cure53 team's perspective, appropriate steps were taken to ensure that good fixes got crafted and now take effect on the RealVNC clients, applications, servers and of course the related backend APIs. The measures proposed and largely implemented as a result of this Cure53 assessment represented necessary steps towards improving the overall security standing of the various objects placed in scope.

Cure53 would like to thank Andrew Woodhouse, Ben May, Richard Allitt, Robert Parsons, Tristan Last, Marc Hull, Tristan Richardson, Andrew Rutterford, Dominic Parkes, and David Doyle from the RealVNC Limited team for their excellent project coordination, support and assistance, both before and during this assignment.