Cure53 Security Assessment of RealVNC Apps, Components & Features, Management Summary, 09.-10.2024

Cure53, Dr.-Ing. M. Heiderich, Dipl.-Ing. A. Inführ, M. Elrod, MSc. N. Krein, MSc. H. Moesl-Canaval, BSc. D. Prodinger, BSc. C. Mayr, MSc. R. Peraglie, MSc. S. Moritz

> *"To conclude, the 2024 assessment results, combined with the 2025 fix verification, confirm that the inspected RealVNC applications within scope are now perceivable as having a strong and stable security posture."*

Cure53, a Berlin-based IT security consulting firm, has been contracted to conduct a penetration test and source code audit of a variety of different RealVNC applications.

The project originated from preliminary discussions held with RealVNC LIMITED representatives in June 2024. Following agreement on the aims and requirements, the assignment received approval, proceeding with a sixty-workday allocation in late September and October 2024. A skill-matched team of nine senior pentesters successfully conducted the technical evaluations.

This initiative sought to appraise the security posture of a number of selected components and features, all of which are itemized in the Work Packages (WPs) below:

- **WP1**: White-box pen.-tests against RealVNC Mobile Server Components
- **WP2**: White-box pen.-tests against RealVNC Single-Sign-On using Azure AD
- **WP3**: White-box pen.-tests against RealVNC API Gateways / Access Keys
- **WP4**: White-box pen.-tests against RealVNC Web-Launcher Implementation
- **WP5**: White-box pen.-tests against RealVNC Presence Implementation
- **WP6**: White-box pen.-tests against RealVNC Portal
- **WP7**: White-box pen.-tests against RealVNC Licensing
- **WP8**: White-box pen.-tests against RealVNC Session (Connection) Audit
- **WP9**: White-box pen.-tests against RealVNC Team Management Audit Service
- **WP10**: White-box pen.-tests against RealVNC WebViewer

Facilitating the white-box methodology, the RealVNC supplied an abundance of assistive materials, such as source code, URLs, mobile applications, test-user credentials, and valuable documentation. A range of key preparation tasks, aimed at ensuring a smooth and efficient project kickoff, were thoroughly concluded in the week prior to the active examination phase, which was CW38.

To facilitate seamless interaction, a dedicated and shared MS Teams channel was established for all RealVNC and Cure53 personnel involved. This collaborative environment ensured a productive process, marked by very few clarifying questions and an absence of general delays. Live reporting was additionally utilized through this platform, providing the developer team with real-time updates and critical observations.

In total, twenty-three findings were identified by the Cure53 auditors throughout the investigation period. This included eight categorized as security vulnerabilities, alongside fifteen documented as common weaknesses that presented a comparatively lower potential for exploitation.

Despite the significant number of tickets and the increased risk associated with some flaws potentially casting a concerning light on the security posture, the initially expansive scope of this engagement meant a larger volume of discoveries was well within expectations. Additionally, the majority of the identified issues are anticipated to be relatively simple to resolve.

Positively, no findings were ranked with a Critical severity rating, and only two were assigned a High impact. This outcome strongly suggests that the RealVNC team has already deployed robust security measures to safeguard their products from severe threats and attacks.

Moreover, the RealVNC team demonstrated commendable responsiveness by initiating the remediation of most findings, including those categorized as High severity, immediately following the conclusion of the test. The resulting implemented fixes were subsequently provided to the Cure53 team, which then meticulously verified their accuracy and effectiveness.

In conclusion, Cure53 is delighted to confirm that, subsequent to the application of the necessary fixes, the assessed RealVNC components now demonstrate a good and improved security posture. Despite this positive development, it remains advisable that all outstanding findings are similarly addressed and remediated promptly to achieve optimal security.

Cure53 would like to thank Ben May, Andrew Woodhouse, Ashley Raven, Neil Gad, Andrew Rutterford, Tristan Richardson, Romeo Kollar, Emma Lewin, Joe Hastings, Conrad Braam, Marc Holloway, and Andrew Spencer from the RealVNC LIMITED team for their excellent project coordination, support, and assistance, both before and during this assignment.