Cure53 Security Assessment of Perdoo Management Summary July 2019

Cure53, Dr.-Ing. M. Heiderich, MSc. S. Moritz, BSc. C. Kean, BSc. J. Hector

Cure53, which is a Berlin-based IT security consultancy, completed a specifically scoped and targeted security assessment of the Perdoo complex. In particular, the project carried out for Perdoo by Cure53 entailed a penetration test, a source code audit, and a dedicated fix verification pursuant to the findings from the initial examination. The main emphasis and objective of this engagement was for the Cure53 to evaluate the Perdoo mobile applications for iOS and Android, as well as their surroundings of the Perdoo server-side API and, last but not least, the web app and admin backend.

From a temporal perspective, it should be noted that the core component of the project, namely the aforementioned penetration test and code review, took place in May 2019. Later on, specifically in July 2019, the Cure53 team approached the scope once more with a task of fix verification. As for the resources, the total budget allocated to this project stood at ten person-days and was split between six members of the Cure53 team involved in the investigation. A methodological lens adopted in this assessment was a so-called white-box approach. This method signified that Cure53 had access to the apps and all relevant sources. Moreover, user-accounts that Cure53 could use for testing on both the production and staging environments were furnished. Exclusively on the stage setup, a super-admin user was also enabled. Notable from the methodological perspective is also the fact that the project progressed in a timely and efficient fashion, with a consistent availability of support from the in-house team at Perdoo. Prompt and productive exchanges in a dedicated, shared Slack channel, positively contributed to the completion of the assessment's goals.

From the breadth of the information and excellent support provided by the Perdoo team, it can be clearly derived that the best possible and wide-spanning coverage was one of the key features achieved by this security project. Cure53 managed to spot six findings on the Perdoo scope in May 2019. These were categorized as three actual vulnerabilities and three general weaknesses. What is crucial to underline is that none of the findings represented major threats. In fact, the highest ranking ascribed to only one issue was set at "*Medium"* severity, indicating that the Perdoo complex could be characterized as having an impressive security posture. The flaws spotted in May 2019 related to the ACL deployment and revolved around the missing enforcement of ACL for *GET* requests, as well as the resulting leakage of data to unprivileged users. Based on this, Cure53 urged the Perdoo team to prioritize the ACL matters going forward. This recommendation appears to have been followed as the Cure53 found all issues to be properly fixed during the verification work conducted in July 2019. All repairs were certified as comprehensive and technically sound, meaning that even minor shortcomings have been eradicated successfully on the Perdoo scope.

Looking at the Perdoo complex more broadly, Cure53 can attest the soundness and robustness that stems from security dedication and making good choices when it comes to frameworks and deployment. For example, the Perdoo web client benefits from the solutions offered by the industry-leading React framework, while other pitfalls are avoided with the help of an HTML sanitizer library. Similarly, the codebase of the applications is kept minimal thanks to the React-Native iteration, again evidencing that simplicity drives exceptional outcomes when it comes to security.

In conclusion, both the testing phase in May 2019 and the successful fix verification carried out by Cure53 in July 2019, confirm that the Perdoo application complex is well secured. As evidenced by the latter stage, the Perdoo team was clearly able to implement the technical feedback and security advice offered by Cure53 to their compound's advantage, thus increasing the already good security posture of the complex. Fine-tuning of the utilized approaches appears to now guarantee consistent and first-rate attack prevention, even if more advanced scenarios and compromise attempts are considered. Finalizing this engagement, Cure53 can confirm that the Perdoo complex incorporates best practices and defense-in-depth concepts correctly. As a result, it exposes no weaknesses subject to exploitation at present.

Dr.-Ing. Mario Heiderich, Cure53, Director, July 9, 2019