Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

Security-Report StartCom Webapp & CMS 03.2017

Cure53, Dr.-Ing. M. Heiderich, MSc. N. Krein, N. Hippert, BSc. D. Weißer, N. Kobeissi

The security assessment of StartSSL was carried out by Cure53 in the first quarter of 2017 in order to identify strength and weaknesses, as well as to provide guidance on improving the overall safety and protections offered by the tested product. It must be emphasized that, being a Certificate Authority (CA), trust and integrity in the security realm are instrumental for the StartSSL project. As CA, StartCom should be perceived as providing a recognized backbone of responsible security for the entire Internet.

The Cure53 security evaluation of the StartSSL suite had a multi-stage design comprising two phases, which were conducted in January and March, respectively. For both phases, a so-called *white-box* methodological approach was chosen, meaning that the Cure53 testers were granted access to all relevant sources and components. After the two main stages, another follow-up fix verification occurred in April 2017. Crucially, between the beginning of testing and the present, the StartSSL has undergone a thorough internal review and consistent overhaul in the areas specified as originally critically lacking. This means that the general verdict accounts for the fact that particular conclusions pertaining to the two testing instances were vastly discrepant.

For the first stage of the assessment, the broadly conceived StartCom compound constituted the main delimitation of the scope, which spanned coverage of three applications (WWW, CMS and backend), various servers and the hosting infrastructure.

A clear rationale for requisitioning the assessment in the first place was the fresh rebuilding of the StartSSL in a new PHP format after suffering critical damage and being deemed untrustworthy by vendors in the past. The security audit was targeted at verifying how the redesigned version fares in the face of modern IT security challenges. Extensive testing in the first phase was completed by a six-member Cure53 team and required a time budget of over twenty-five working days. In sum, the results of the tests were catastrophic: not only was a high number of twenty-seven different security vulnerabilities and general weaknesses discovered, but as many as ten issues among them were classified to be “Critical” in terms of scope and severity. This translated to a very high percentage of the total findings threatening the very core of the project’s security and integrity, as well as suggested haste and organic development. What is more, the findings were underpinned by or interlinked with structural problems affecting the application. The flaws related to the application’s code, code design, framework integration, cryptographic implementations, deployment practices and other issues, thus signaling a plethora of distinct problems plaguing the tested scope of the StartCom.

Dr.-Ing. Mario Heiderich, Cure53
Rudolf Reusch Str. 33
D 10367 Berlin
cure53.de · mario@cure53.de

Given the purpose of the application, the results of the first stage of the assessment warranted paramount concerns about the chances of moving forward as the assessment concluded. The Cure53 testing team clearly stated that the lack of security at StartCom did not allow for a deployment into production.

Against the first stage's negative outcome, the second round of the assessment took place two months later, this time involving five Cure53 testers for a shorter period of ten days. While ten new security-relevant issues were identified, the primary goal was to verify the fixes deployed by StartCom in response to the discoveries made in the previous phase. On the latter, it has to be noted that only one issue among the January 2017 findings was determined to lack sufficient handling and a proper fix. Other technical shortcomings were addressed correctly. Further, in April 2017, there was a follow-up round of fix verification for the cumulative findings of both testing rounds, which once again reflected the tremendous progress in the overall level of the application security. Ultimately, all of the issues identified by Cure53 were resolved and met with appropriate fixes.

In conclusion, it is evident that the time between the two rounds of testing and since the assessment concluded was well-spent by the StartCom maintainers. The overall leap in the state of security is considerable and very much praiseworthy. At present, the ultimate improvement stems from solid dedication to fixing the reported problems appropriately and in a manner that prevents recurrence. As two most important arguments, it can be noted that the numbers of bugs decrease significantly and that the vast majority of the previously spotted issues has been addressed correctly. The current tendency towards improvement can be read as a good sign. With each passing month, dedication to security appears to grow and positively affect the StartSSL compound.