Fine penetration tests for fine websites

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

Cure53 Assessment of the AdNovum NEVIS Security Suite - Management Summary 12.2018

Cure53, Dr.-Ing. M. Heiderich, N. Hippert, MSc. N. Krein, BSc. T.-C. “Filedescriptor” Hong, BSc. J. Hector, MSc. D. Weißer

The maintainers of the AdNovum NEVIS Security Suite commissioned Cure53, a Berlin-based IT security consultancy, to perform an assessment of their products security posture in 2018. Aiming at gaining a better picture from a perspective of an external, as well as potential internal adversaries, this project spanned both a penetration test and a source code audit of the pre-selected items in the AdNovum NEVIS Security Suite’s scope.

Going beyond the general target of the AdNovum compound, the project focused on three specific items, namely the NEVIS Security Suite’s reverse proxy, NEVIS Security Suite’s authentication premise and, last but not least, broader authentication mechanisms, protocols and designs created and deployed by NEVIS. In terms of resources, the tasks were given to a team comprising six members of the Cure53 team. They were allocated a time budget of fourteen days and the majority of work was invested into the core investigations taking place in October 2018.

The assessment relied on a number of methods, but primarily concerned an in-depth analysis of the provided sources, as well as running stress tests and fuzzing tools against the builds furnished by the AdNovum maintainers. Consequently, a white-box approach was adopted here and Cure53 was furnished access to sources via the AdNovum file-sharing platform. Moreover, extensive documentation was also shared with the testing team. Having said that, the application provides an extensive feature set, so only a small subset of all aspects could be evaluated during this audit. The items were filtered by relevance and exposure, with the main focus placed on the NEVIS proxy component.

Fast progress was made by Cure53 on the scope during Calendar Weeks 41 and 42. Since all communications with very professional AdNovum project team were done in a private Slack channel, the complexities of the source and documentation pile could be quickly explained. The investigations led to seven security-relevant discoveries being made on the scope. It must be emphasized that the majority of the findings belong to the category of general weaknesses and posed limited threats. It was also ascertained that the sole vulnerability spotted on the scope carried a “*Medium”* security ranking only. In other words, no problems that could be deemed as triggering “*Critical”* or even just “*High”*-ranking risks could be unveiled.

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

Despite intensified efforts from the Cure53 team, no major defects like Remote Code Execution, privilege escalation or authentication bypasses could be found on the AdNovum scope. The main concern still lies in the fact that a great portion of the deployed code has been directly copied from open source projects without further updates, so Cure53 continues to advise an in-depth and step-by-step analysis of this realm. With this in mind, it is also believed that patch management should be prioritized going forward. Being such a complex project, AdNovum might similarly require in-house fuzzing and audits to remain safe internally.

Among the findings, the flaws expectedly concerned outdated patterns and items. For instance, security protocols in use relied on older cryptographic functions (e.g. SHA1, sometimes MD5), which are still considered secure, yet are becoming deprecated and should be replaced with newer algorithms. It needs to be clearly stated, however, that the AdNovum team reacted to the findings and engaged in crafting fixes. The most concerning finding was addressed in full and the Cure53 team verified the approach as viable and correct. In the next stages, the issues with low-severities will be tackled in due course as part of the next release.

To sum up, given the complexity of the AdNovum NEVIS Security Suite, as well as the age of some of the sources, Cure53 was positively surprised in how well security has been managed in the tested compound. Based on the findings, the Cure53 team could only conclude that the AdNovum NEVIS Security Suite emerged victorious from this 2018 security assessment. The achieved outcomes – in terms of both the low number and limited severities of the findings – are rare and praiseworthy.