Fine penetration tests for fine websites

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

Pentest-Report DeepL Infrastructure & K8s 11.-12.2022

Cure53, Dr.-Ing. M. Heiderich, J. Larsson, M. Elrod

Index

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

Introduction

"With DeepL, you'll never have to compromise on quality again. Powered by neural networks and the latest AI innovations, our technology captures even the slightest nuances and reproduces them in translation, unlike any other service. Our translations are proven to be over 3 times more accurate than our closest competitors."

From https://www.deepl.com/en/why-deepl-pro

This report describes the results of a penetration test and security assessment against the DeepL infrastructure and Kubernetes (K8s) deployment. Carried out by Cure53 in late 2022, this project has been registered as *DPL-02.*

As for the precise timeline and specific resources, the work was requested by DeepL SE in June 2022 and scheduled for the end of 2022, allowing sufficient time for preparations on both sides. Cure53 completed the project in late November and early December 2022, namely from CW46 to CW48. A total of nine days were invested to reach the coverage expected for this project and the assessment was conducted by three senior testers from the Cure53 team.

The work was contained into a single work package (WP):

- **WP1**: Penetration-tests and security assessments against DeepL infrastructure and K8s

Cure53 was provided with details about the infrastructure, test-users, as well as all means of access required to complete the tests. More importantly, the DeepL team shared a list of attack-scenarios for the test, thus guiding the phases of this project. The methodology chosen here represents a so-called gray-box.

All preparations were done in November 2022, namely CW45. This meant Cure53 could have a smooth start and proceeded fluently with the testing efforts. Communications during the test were done using a dedicated shared Slack channel set up to connect the DeepL SE and Cure53. All involved personnel from both parties could participate in the discussions happening on Slack.

The discussions throughout the test were very good and productive and not many questions had to be asked. Ongoing interactions positively contributed to the overall outcomes of this project. The scope was well-prepared and clear, greatly contributing to the fact that no noteworthy roadblocks were encountered during the test.

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

Cure53 gave frequent status updates about the test and the related findings. Live-reporting was not specifically requested and it would not have been necessary given the short list and limited implications of the spotted findings.

The Cure53 testing team managed to get very good coverage over the scope. Only three discoveries, all in the realm of general weaknesses with lower exploitation potential, could be made. This clearly signifies a very small range of issues and can be interpreted as a very good sign in regard to the security of the DeepL infrastructure. Foreshadowing conclusions, it can be derived from above that DeepL be congratulated on achieving a very good level of security for their infrastructure and K8s.

The report will now shed more light on the scope and test setup as well as the available material for testing. This section will be followed by a chapter that details the test methodology used in this exercise. This is to show which areas of the complex in scope have been covered and what tests have been executed despite only a handful of actual findings to report.

Flaws categorized as general weaknesses will then be listed chronologically. Each finding will be accompanied with a technical description, a PoC where possible, as well as mitigation or fix advice. The report will then close with a conclusion in which Cure53 will elaborate on the general impressions gained throughout this test, reiterating the verdict about the perceived security posture of the DeepL infrastructure, K8s setup and deployment.

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

Scope

- **Penetration tests & Security assessments of DeepL infrastructure & K8s**
  - **WP1**: Penetration tests & Security assessments of DeepL infrastructure & K8s
    - **Test-users and infrastructure:**
      - **Granted access:**
      - **K8s cluster:**
      - **K8s namespaces:**
      - **K8s users:**
    - **Attack Scenario 1**
      - An attacker who has gained access to the network but does not have k8s access at all
      - The focus was on breaking into k8s (but not on compromising the applications running on k8s)
    - **Attack Scenario 2**
      - A rogue developer accessing resources in a development namespace
    - **Attack Scenario 3**
      - A rogue developer accessing resources in a *"production"* namespace
    - **Attack Scenario 4**
      - An application where a security vulnerability leads to a *shell* inside a pod - possible consequences.
  - **Test-supporting material was shared with Cure53**
  - **All relevant sources were shared with Cure53**

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

Conclusions

To reiterate, this security assessment targeted the DeepL complex, specifically the DeepL Kubernetes cluster and the attached infrastructure. It can be concluded that the results of this Cure53 2022 project unequivocally indicate that the security premise of the tested complex is robust and well-thought-out. The Cure53 team - which consisted of three members and spent nine days examining the test-targets, found no actually exploitable security vulnerabilities within the scope. Only a few general weaknesses and notes on further hardening could be shared.

During the whole assignment, Cure53 maintained frequent contact with the DeepL team. The support at the DeepL was - without exception - extremely fast, competent and helpful. It was consistently offered whenever the Cure53 testers had questions regarding the engagement.

Notably, the assessment was divided into four scenarios, each simulating different attacks and attacker perspectives. This was carefully planned in order to maximize coverage of different breach scenarios. Consequently, the testing process included a wide array of components. Many of these components further exposed a multitude of configuration options and shall be reflective of adherence to best practices.

A theme that prevailed throughout the test was that all checked options were configured properly and with security in mind. This by itself is very impressive in Cure53's view. The overall security concepts adopted by DeepL should be regarded as very good and well-implemented. Furthermore, the overall defense-in-depth and least-privileged concepts were observably guiding the deployment of the examined infrastructure.

The current configuration was analyzed for common insecure defaults, misconceptions as well as misconfiguration issues. The presence of three *Miscellaneous* findings does not detract from a perception of high level of security awareness within the DeepL team. Separation concepts and hardening efforts observed during scenarios 1 and 2 should be regarded as solid.

During attack scenario 3, it was tested what impact a rogue developer could have on the security landscape, with special attention to how their access was being restricted. Fully and effectively locking down this access while still keeping the setup practical is by no means a simple task. It was nevertheless fully mastered by the DeepL engineers. This conveys confidence not only in the engineering practices, skills and methodologies applied, but also paints a good picture of the planning and organization processes. It shows that the developers have taken the time needed to properly set up the software and securely lock down all components.

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

The only topic that was not found to be fully optimized was encountered in scenario 4 and pertained to somewhat insufficient network isolation. While it did not lead to any Kubernetes compromise, Cure53 has found a possibility to reach several internal services over the network. Once this has been addressed, it is fair to say that DeepL network and cloud setups should be judged as properly secured in the scenario 4's context.

When inspecting the internal services, it was also noticed that an attacker who had initial access to an app running in the development network could join Zoom meetings. DPL-02-003 illustrates this but the fact that this finding was the most severe showcases how well-designed, built and maintained all of the inspected infrastructure components were.

In order to summarize this 2022 security assessment, Cure53 must state that the DeepL infrastructure should be considered as very well-implemented and aligned with common security standards. The DeepL team's successful efforts towards building and putting forward an absolutely convincing self-hosted cloud setup are definitely praiseworthy.

Cure53 would like to thank Daniel Forster, Sean Mitchell, Tim Buchwaldt and Kai Kunschke from the DeepL SE team for their excellent project coordination, support and assistance, both before and during this assignment.