FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš
Student:	Vojtěch Krejsa
Thesis title:	Analysis of the Zlib's CVE-2022-37434 Vulnerability
Branch / specialization:	Computer Security and Information technology
Created on:	20 May 2023

Evaluation criteria

1. Fulfillment of the assignment

▸ [1] **assignment fulfilled**
[2] assignment fulfilled with minor objections
[3] assignment fulfilled with major objections
[4] assignment not fulfilled

The assignment of the thesis is unusually difficult for a Bachelor level as it requires a fairly deep exploration of low level data structures. Even the majority of Master level students would probably find it quite challenging. The student wasn't satisfied with that and certainly went above and beyond, because he didn't complete just the assignment as written, but did it for two very different operating systems with significantly different behavior in their memory manager. Essentially, he performed a work that would usually take two full Master Theses.

2. Main written part 100/100 (A)

The written part of the thesis is very nearly perfect. I did notice a few minor typos (e.g. "priviledges" in one place), but other than that, I can only praise it. It correctly describes the necessary preliminaries, including the vulnerabilities in general and the buffer overflows and their properties specifically as well as the background for the relevant parts of the Zlib library. Then the analysis of CVE-2022-37434 begins, first with the known information and then the new extensions that go very deep into the internals of Zlib and the behavior of the heap, finally leading to a successful remote code execution on two different operating systems.

3. Non-written part, attachments 100/100 (A)

The non-written parts consist of the proof-of-concept applications for Ubuntu and Windows 10. A virtual machine with a ready-to-try PoC for Ubuntu is also provided. The reader can easily try it out on their machine. My only complaint is that the network cable could have been left unplugged for the virtual machine.

4. Evaluation of results, publication outputs and awards 100/100 (A)

The student analyzed a recent vulnerability (just a few months old at the time of starting the thesis) and significantly extended its understanding. Beyond just showing how exactly it works, he was also the first who managed to demonstrate the remote code execution inherent in it that was heretofore suspected but never actually proven.

5. Activity of the student

▸ [1] **excellent activity**
[2] very good activity
[3] average activity
[4] weaker, but still sufficient activity
[5] insufficient activity

6. Self-reliance of the student

▸ [1] **excellent self-reliance**
[2] very good self-reliance
[3] average self-reliance
[4] weaker, but still sufficient self-reliance
[5] insufficient self-reliance

The overall evaluation 100/100 (A)

Overall, this is an excellent work. The student came up with a recent and challenging topic and handled it in an exemplary manner, significantly extending the previous knowledge of the Zlib vulnerability. That he was able to perform remote code execution not on just one but two different operating systems at the Bachelor level is nothing short of amazing. This is definitely a work worth considering for the Dean's Prize. I am happy to recommend it for defense and grade it A-excellent.

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.