FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. Martin Kolárik
Student:	Jakub Ferjak
Thesis title:	CVE-2023-37903: Remote Code Execution vulnerability in the vm2 library
Branch / specialization:	Information Security 2021
Created on:	11 June 2024

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

2. Main written part 95 /100 (A)

The written part is very comprehensive and provides the necessary background, even for readers with little to no knowledge of JavaScript or computer security. Despite its length, it is factually precise and very well-written. The sources used are appropriate and properly cited.

3. Non-written part, attachments 95 /100 (A)

The attachments include code samples for scenarios discussed in the text and a simple web application that allows code to be executed in the selected sandbox. The application makes it easy to verify the results or perform further experiments.

4. Evaluation of results, publication outputs and awards 85 /100 (B)

The thesis does not present any new findings, but its detailed description of the vm2 vulnerability and the overview of alternative JavaScript sandboxing libraries could be useful for security professionals or JavaScript developers trying to understand the security aspects of various sandboxing techniques.

The overall evaluation 95 /100 (A)

Both the written and non-written parts are of excellent quality, so it only fits to grade this as 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.

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.