UMEÅ UNIVERSITY

Talos+ Leveraging Structured Error Handling For Increased Security

Broad software vulnerability mitigation through enabling Security Workarounds for Rapid Response in Java

Melker Henriksson

Melker Henriksson
Spring 2025
Degree Project in Interaction Technology and Design, 30 credits
Supervisor: Prof. Alexandre Bartél
External Supervisor: Anders Sigfridsson, Evelina Malmqvist
Examiner: Ola Ringdahl
Master of Science Programme in Interaction Technology and Design, 300 credits

Abstract

The pre-patch window of Vulnerability remains a critical challenge in cybersecurity, leaving systems exposed to exploits before patches are deployed.

The paper *'Talos: Neutralizing Vulnerabilities with Security Workarounds for Rapid Response'* by Zhen Huang et al. proposes an algorithm that detects error-handling code and instruments it with security workarounds, allowing developers to disable vulnerable segments temporarily.

This thesis aims to extend, compare, and verify the claims made in the Talos paper. Since the algorithm's heuristics focus on languages without structured exception handling and experiments are only performed on programs written in c/c++, there is as mentioned in future works potential to expand Talos functionality to cover these languages.

By extending Talos to Java, this research strengthens its viability as a mitigation strategy and provides a proof of concept for its applicability in languages with structured exception handling.

The findings aim to improve the pre-patch vulnerability window for Java and explore potential Vulnerabilities resulting from Talos and so contribute to the broader field of cybersecurity.

Acknowledgements

Contents

1 Introduction

before the first chapter.

References