Coverity Scan Static Analysis Report

Hardhard Enterprises

**T1** 2023

Statement of Intent

Overview

This document aims to provide a record of static code analysis performed on a specific issue from the Coverity SAST scan for the NASA ION Open-Source code 4.1.1 project.

The primary purpose of this document is to validate the issue identified via the automated detection process to eliminate false positives.

Depending on findings, secondary purposes can include but are not limited to listing/providing recommended fixes alongside a list of attack vectors and potential exploits for consideration.

Reporting Best Practices

Please ensure best practices are kept when completing the document via regularly updating the Acronyms and Abbreviations table alongside any iterations made to the Document History table. This will allow other members to identify any updates and progress made across trimesters easily.

When using code snippets, please use screenshots that are clear and easy to read, alternatively, use words built-in code formatter found [here](https://appsource.microsoft.com/en-us/product/office/WA104382008?tab=Overview).

Document Naming Conventions

Naming conventions for this file are as follow; SAR\_{CID}. For example, when investigating issue 123456 the file name would be SAR\_123456.docx

Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Dates** | **Version** | **Author** | **Comments** |
|  | V0.1 |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Content

Contents

[Introduction 3](#_Toc119848724)

[Objective 3](#_Toc119848725)

[Scope 3](#_Toc119848726)

[Acronyms and Abbreviations 3](#_Toc119848727)

[Code Review and Analysis 4](#_Toc119848728)

[Outcomes 4](#_Toc119848729)

[Observations 4](#_Toc119848730)

[Supporting Evidence 4](#_Toc119848731)

[Conclusions and Recommendations 4](#_Toc119848732)

[References 5](#_Toc119848733)

[Appendix 6](#_Toc119848734)

# Introduction

## Objective

The primary objective of this analysis is to determine whether the defects identified in the Coverity Report for the ION Open Source 4.1.1 project are:

* Indeed, defects.
* Potentially exploitable.

The secondary objective of this analysis, where applicable, is to provide the following:

* Recommendation(s) to fix.
* Any exploit for consideration.

## Scope

This static code analysis is limited to the ***untrusted loop bound***  type defect identified in the following CIDs:  
***1520698.***

# Acronyms and Abbreviations

Please keep an updated list of acronyms and abbreviations used throughout the report.

|  |  |
| --- | --- |
| **Acronym** | **Meaning** |
| DTN | Delay/Disruption Tolerant Network |
| ION | Interplanetary Overlay Network |
|  |  |

# Code Review and Analysis

## Outcomes

The report outlines the observations of CID 1520698, a untrsusted loop bound defect.

## Observations

*A screenshot of a computer

Description automatically generated*Coverity is finding an untrusted loop-bound defect. This shows that there is a loop in the code where the loop bounce – the value that determines how many times the loop will go – is considered untrusted.

The TAINTED\_SCALAR label means that the value may come from a poorly sanitised source before being used in the loop.

The tainted\_data part indicates that there is a variable or expression that is considered tainted by Coverity. This means that the data comes from an untrusted or external source and hasn’t been validated or sanitized to ensure it is safe to use. The data is being passed as an argument to tolocal and is using the tainted expression as a loop boundary – determining how many times a loop inside will run.

# Conclusions and Recommendations

This can be a source of vulnerabilities like buffer overflows, infinite loops, or other unexpected behaviour if the tainted data isn’t properly validated before being used as a loop band.

The code where the error occurred should be reviewed to address this issue. This will ensure any data coming from untrusted sources is properly validated and sanitised before being used in a loop boundary and potentially consider using safer constructs or methods to control your loops to prevent security vulnerabilities.