**T1** 2023

Coverity Scan Static Analysis Report

Hardhard Enterprises

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** |
| 25/04/2023 | V0.1 | Anthony Scantsonihas | Beginning of the investigation |
| 26/04/2023 | V0.2 | Anthony Scantsonihas | Investigation |
| 27/04/2023 | V1.0 | Anthony Scantsonihas | Finalization |

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 ***Use of 32-bit time\_t*** type defect identified in the following CIDs:  
***CID 1520764***

# 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 |
| CID | Coverity Issue Identification Number |
| CWE | Common Weakness Enumeration |

# Code Review and Analysis

## Overview

The Coverity flag for the CID 1520764 has found an issue within the code base brsscla.c392. The error being flagged is a use of 32-bit time issue which is found under CWE-197. This issue is also know as a Numeric Truncation Error and it occurs when a mathematical operation is performed using a finite number of digits, and the result is rounded to fit that limited number of digits therefore preventing the result from being entirely accurate.

## Observations

The error appears to arise from the recieveBundles function which acts as the main loop for a bundle reception thread on one connection. This means that the function receives bundles and then terminates them when the connection is lost.

Graphical user interface, text

Description automatically generated

As can be seen within the screenshot above there appears to be three instances of the issue occurring within the function. The errors seem to revolve around the time\_t variable having a insufficient number of bits to represent it causing the value to be truncated and thefore potentially causing a loss of information as well as incorrect results within the program.

## Supporting Evidence

Screenshots of these three errros can be found below. These screenshots demonstrate how the time\_t value is the main cause for the issue found within this CID.







# Conclusions and Recommendations

In conclusion it is unlikely that these errors can be exploited by an attacker to perform malicious actions upon the program. However, they may indicate potential underlying weaknesses found within the code that could be further exploited.

My recommendation for solving this issue would be to implement a larger integer data type for the time\_t variable, as doing so would allow for the program to store the variable without the negative effects of truncation.

References  
Please keep an updated references list in APA7; The Deakin referencing guide can be found [here](https://www.deakin.edu.au/__data/assets/pdf_file/0009/2236752/Deakin-guide-to-APA7.pdf).

WE-197: Numeric Truncation Error. (2023, April 20). Retrieved from Common Weakness Enumeration: https://cwe.mitre.org/data/definitions/197.html

Appendix

Include additional information/documentation here to help the readers understand complex information.