Coverity Scan Static Analysis Report

Hardhard Enterprises

**T3** 2022

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 formatted 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** |
| 20/11/2022 | 1 | Jesse Ludeman | Initial document |
|  |  |  |  |
|  |  |  |  |

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 4](#_Toc119848733)

[Appendix 4](#_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 ***High impact quality*** type defect identified in the following CIDs: 1520895

# 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

When performing static code analysis using the ION Open Source 4.1.1 dashboard for CID 1520895, there is a high impact problem that involves the use of 32-bit time\_t function. The Coverity scan tool has indicated that on line 882 an unsigned integer is being used to store a time value.

## Observations

An unsigned integer is a 32-bit datum that encodes a non-negative integer in the range of [0 – 4294967295]. The issue here is that if a primitive data structure is passed a value that is bigger than what it can store, the program can lose data in the process. Therefore, if the atTime function receives a value that the unsigned integer data type cannot store, this can cause an issue with the program’s execution.

There is currently no vulnerability associated with this issue.

## Supporting Evidence

|  |
| --- |
| CHKERR(bundle && bundleObj && terminusNode);  TRACE(CgrBuildRoutes, terminusNode->nodeNbr, bundle->payload.length,  (unsigned int) atTime); |

# Conclusions and Recommendations

To resolve this problem, the solution would be to cast the atTime function to a signed integer data type. A signed integer can hold both negative and positive numbers. This would then need to be tested to ensure the code is still valid.

References

Appendix

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