**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** |
|  | 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 ***{Issue Category}*** type defect identified in the following CIDs:  
***{Coverity Issue CID}***

# 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

## Overview

Looking at CID-1520859. This is an **Out of Bounds access** error. This is also referred to as a buffer overflow or a memory safety error. Essentially this means that the code is able to read and write from outside the boundary of the buffer intended.

## Observations

This error seems to be occurring when assigning the “elt” variable with the “SM\_list\_data” variable.



This is a very large index of numbers that may include negative parametres that can be interpreted as unassigned.

If the memory that is out of bounds can be accessed by a potential attacker, it can essentially be controlled by the attacker. The attacker can then possibly execute code fragments and modify the memory within the code.

This will also likely lead to corruption of the relevant memory as well as potentially having the program be repeated in an infinite loop.

If the attacker has access to an Out of bound read then they may have access to sensitive information within the system and program. Which can then lead to further consequences throughout the system.

## Supporting Evidence

https://cwe.mitre.org/data/definitions/119.html

# Conclusions and Recommendations

This is an incredibly high risk error that needs to be amended immediately. An attacker having access to this error could be dire for the system. The recommendation is to attempt to fix the out of bound access and have the program only access the required memory.

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).

https://cwe.mitre.org/data/definitions/119.html

Appendix

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