**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** |
| 19/09/2023 | V0.1 | Anthony Scantsonihas | Beginning of investigation |
| 20/09/2023 | V0.2 | Anthony Scantsonihas | Researched the error 'Function call with incorrect argument type' |
| 21/09/2023 | V0.3 | Anthony Scantsonihas | Began report write up |
| 22/09/2023 | V.1.0 | Anthony Scantsonihas | Completed report write up |

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 ***1520865*** type defect identified in the following CIDs:  
***Function Call with Incorrect Argument Type***

# 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 system has identified an issue within the code base ui\_input.c:299, this issue being a Function Call with Incorrect Argument Type error which is under CWE-686. The issue indicates that there is a component in the code where the caller specifies an argument with the incorrect data type causing the program to crash.

## Observations

The primary issue stems from the “uint8\_t” function where there is a type mismatch in the ‘printf’ format specifier when printing the length of the hexadecimal blob.

A screenshot of a computer program

Description automatically generated

**-Potential Vulnerabilities**

Overall, from what can be seen within the Coverity flag the code does not appear to contain any significantly exploitable vulnerabilities. However, it is important that the error caused from this issue is handled effectively.

## Supporting Evidence

A screenshot of a computer program

Description automatically generated

# Conclusions and Recommendations

In conclusion, my recommendation to alleviate this issue would be to implement input validation and effective error management, as doing so would help to prevent errors when there are unexpected data types being utilized within the program.

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).  
MITRE Corporation. CWE - CWE-686: Function Call With Incorrect Argument Type. From <https://cwe.mitre.org/data/definitions/686.html>

Appendix

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