**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** |
| 15/09/2023 | V0.1 | Anthony Scantsonihas | Beginning of investigation |
| 16/09/2023 | V.02 | Anthony Scantsonihas | Researched the error type 'Ignoring number of bytes read' |
| 17/09/2023 | V.03 | Anthony Scantsonihas | Began report write up |
| 18/09/2023 | V1.0 | Anthony Scantsonihas | Finalized 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 ***Ignoring number of bytes read*** type defect identified in the following CIDs:  
***CID 1520790***

# 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 discovered an issue within the codebase platform.c3347. The issue is an unchecked return value where the code ignores the number of bytes read when conducting one of its functions. This means that the number of bytes copied into the buffer can potentially be smaller than the requested number of bytes therefore allowing the buffer to potentially be accessed out of range.

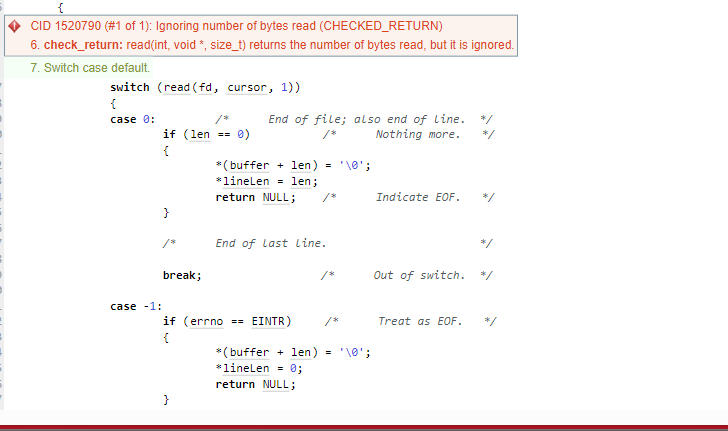
## Observations

The code flagged for this CID appears to be responsible for the function of reading lines from a file descriptor when error handling. The error stems from the “\*igets” function where there is a call to the ‘read’ function within a switch statement but the return value of ‘read’ is neither being used nor checked by the program. The error message appears as a warning indicating that this oversight within the code may lead to unintended behavior.

**-Potential Vulnerabilities**

Whilst this segment of code alone doesn’t provide any large direct security vulnerabilities, it still may contribute to security issues for the overall program as the insufficient handling of errors and unvalidated inputs can lead to potentially dangerous outcomes for the security of the service.

## Supporting Evidence



# Conclusions and Recommendations

In conclusion of this investigation, my recommendation to resolve the issue would be to implement proper error handling and resource management techniques as well as input validation. Doing so would ensure that if the processes are to encounter variables containing unexpected values the program will remain relatively stable and not be vulnerable to unexpected outputs that may cause the program to crash.

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-252 Unchecked Return Value. From <https://cwe.mitre.org/data/definitions/20.html>

Appendix

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