**T2** 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** |
| 6/09/2023 | V0.1 | LIANG CHEN | Analyze Improper Input Validation |
|  |  |  |  |
|  |  |  |  |

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 5](#_Toc119848732)

[References 6](#_Toc119848733)

[Appendix 7](#_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 ***Improper Input Validation*** type defect identified in the following CIDs:  
***1520835***

# 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

## This report focuses on the error analysis of CID:1520835 within the decodeBundle function found in the libbpP.c file. Specifically, the warnings raised in error six and eight associated with sdr->dssm. They seem to pertain to data that might be unsafe or "tainted."

## Observations

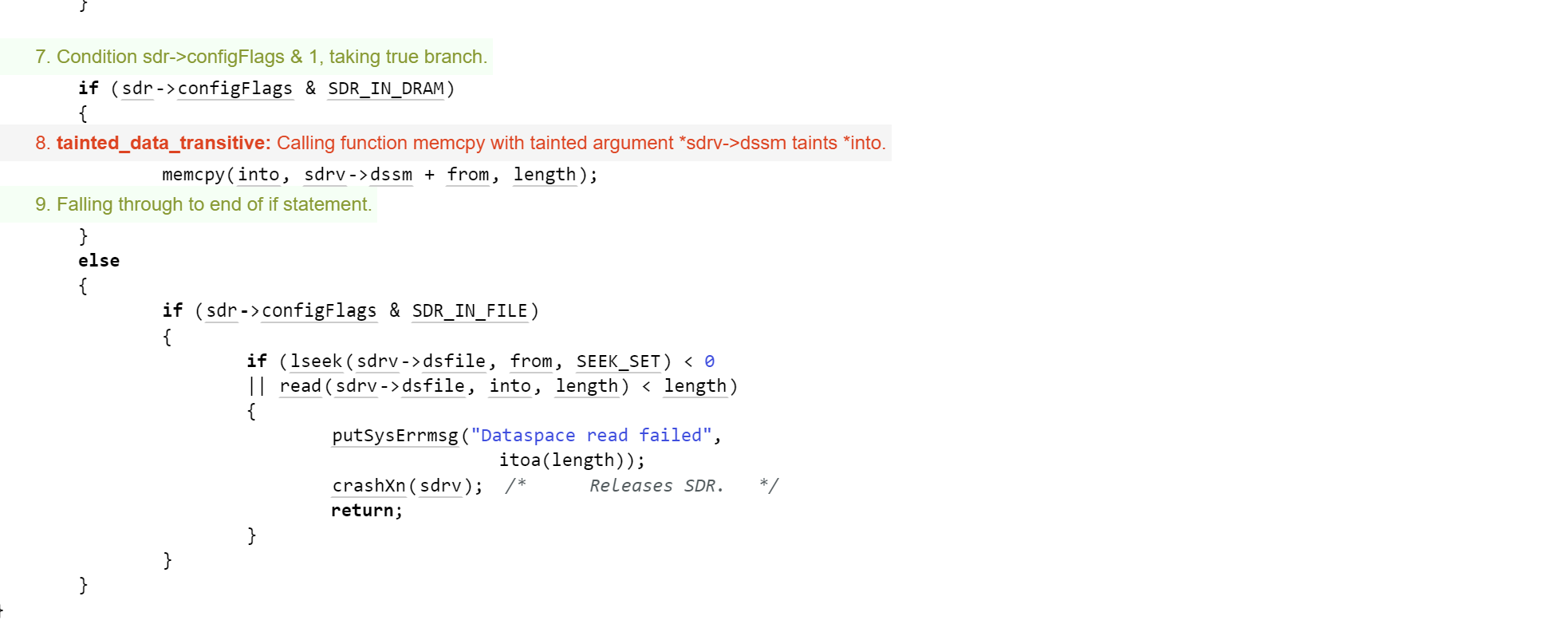
## Both error six and eight relate to tainted data, emphasizing the possibility that the program might process untrusted or compromised data. From the details, we can discern that these two errors are raised by the \_sdrput and \_sdrfetch functions. The tainted data might either be passed to these functions or be returned by them, leading to potential security vulnerabilities.

## Supporting Evidence

## 1



For error 6:Within the \_sdrput function located in /ici/sdr/sdrxn.c, the function call memcpy(sdrv->dssm + into, from, length); apparently taints the sdrv->dssm parameter, as indicated by the tainted\_data\_transitive warning. This suggests that data within sdrv->dssm might be polluted by potentially untrusted sources.



For error 8:In the \_sdrfetch function found in /ici/sdr/sdrxn.c, the function call memcpy(into, sdrv->dssm + from, length); seems to pass a tainted sdrv->dssm value, as shown by the tainted\_data\_transitive warning. This could raise concerns if the sdrv->dssm parameter influences memory read/write operations without validation.

# Conclusions and Recommendations

Both error six and eight relate to tainted data, emphasizing the possibility that the program might process untrusted or compromised data. From the details, we can discern that these two errors are raised by the \_sdrput and \_sdrfetch functions. The tainted data might either be passed to these functions or be returned by them, leading to potential security vulnerabilities. It's recommended to inspect the implementations of \_sdrput and \_sdrfetch to identify and mitigate the source of the tainted data.

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).

7 Pernicious Kingdoms (CWE Draft 3, 2006-07-19, Submitted on July 19, 2006).

<https://cwe.mitre.org/data/definitions/20.html>

Appendix

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