.





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 | Kanad Dombhare |  |
|  |  |  |  |
|  |  |  |  |

Table of Content

Contents

[Introduction 3](#_gjdgxs)

[Objective 3](#_30j0zll)

[Scope 3](#_1fob9te)

[Acronyms and Abbreviations 3](#_3znysh7)

[Code Review and Analysis 4](#_2et92p0)

[Outcomes 4](#_tyjcwt)

[Observations 4](#_3dy6vkm)

[Supporting Evidence 4](#_1t3h5sf)

[Conclusions and Recommendations 4](#_4d34og8)

[References 5](#_2s8eyo1)

[Appendix 6](#_17dp8vu)

# 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 ***“untrusted value as argument”*** type defect identified in the following CIDs:  
***1520669***

# 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

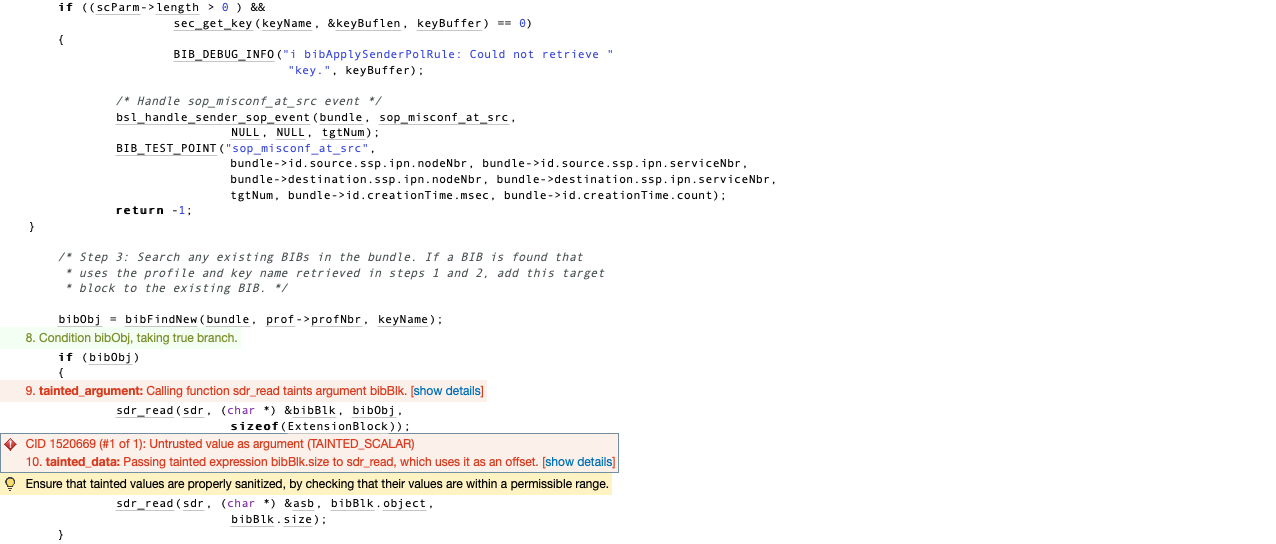
The code sample provided is part of a bigger program including security and data processing, specifically the Bundled Protocol (BP) and Bundled Protocol Security (BPSec) libraries. The code looks to be a function in charge of implementing a sender policy rule on a bundle. It entails different checks, event processing, and interactions with data structures linked to security.

## Observations

According to CWE-20 Improper Input Validation

The product receives input or data, but it does not validate or verifies wrongly that the input has the attributes required to process the data securely and correctly.Input validation is a common technique for ensuring that potentially harmful inputs are safe for processing within the code or when dealing with other components. When software fails to properly validate input, an attacker can craft input that is not expected by the remainder of the application. This will result in unexpected input to components of the system, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution.

## Supporting Evidence



# 

The code exhibits a comprehensive approach to error handling and security by meticulously checking for NULL pointers and meticulously validating diverse parameters associated with both data integrity and security. It raises noteworthy apprehensions concerning tainted data, particularly its utilization within the sdr\_read function. The code's comments aptly underscore the inherent risks and potential issues linked with such data. The script adeptly manages the retrieval of BIB profiles and security context parameters while adeptly addressing instances where these values are absent. Additionally, the code adeptly processes BIB objects, which could involve extracting data and leveraging their attributes. Notably, the implementation includes event handling mechanisms, tailored for distinct situations like misconfigured security and debugging, reinforcing the code's responsiveness to various scenarios.

# 

# Conclusions and Recommendations

To bolster the security and reliability of the code, several key measures should be taken. First and foremost, addressing the issue of tainted data is imperative; this involves meticulously sanitizing tainted values prior to their utilization in critical functions such as **sdr\_read**. Ensuring memory safety is equally vital, necessitating the validation of data, particularly values like **bibBlk.size**, in order to forestall potential threats such as buffer overflows or unauthorized memory access. Augmenting error handling through comprehensive logging and debugging mechanisms is advisable, as this practice aids in efficiently diagnosing and resolving runtime issues. To streamline code maintenance and minimize redundancy, a strategic reconsideration of event handling is recommended, with the potential to centralize this process. Lastly, guarding against security vulnerabilities is paramount. Achieving this entails robust input validation for user-supplied data to prevent risks like buffer overflows. By conscientiously adhering to these recommendations and adhering to security-conscious practices, the code's integrity and dependability can be significantly heightened, aligning it more closely with the intended goals of safeguarding data and ensuring secure operation.

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)*.*

Appendix

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