



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** |
| --- | --- | --- | --- |
| 27/08/2023 | V0.1 | Kanad Dombhare | Initial Document |
|  |  |  |  |
|  |  |  |  |

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 ***Structurally Dead Code*** type defect identified in the following CIDs:  
***1520789***

# 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 |
| CWE | Common Weakness Enumeration |
| BIB | Bundle Integrity Block |

# Code Review and Analysis

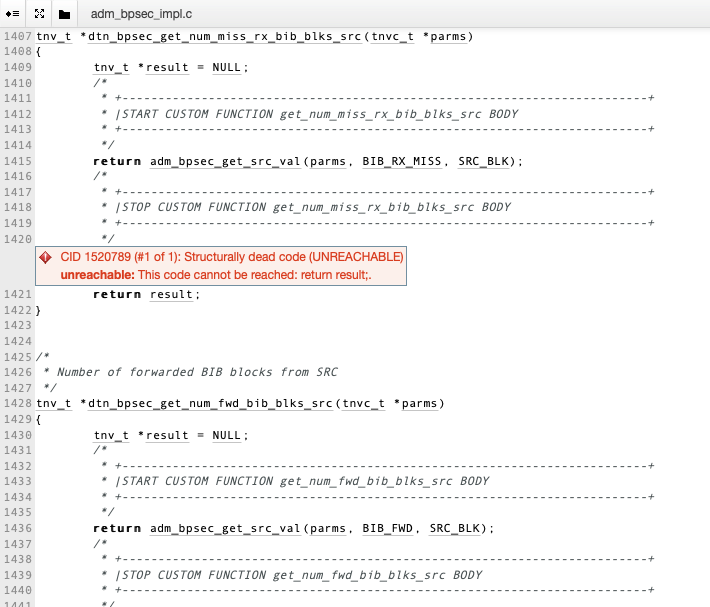
## Overview

While examining the code in the "adm\_bpsec\_impl.c" file located in the administration (adm) folder of the Bundle Protocol v7 directory, an issue was identified by Coverity. This issue involves a "Structurally Dead Code" error flagged at line 1421 in the function named **dtn\_bpsec\_get\_num\_miss\_rx\_bib\_blks\_src**. This error signifies the presence of code that cannot be executed. The mentioned function is responsible for gathering the most recent BPSEC update from the source node.

## Observations

The function seems to serve a specific purpose related to retrieving the number of missing blocks on the receiving end from a source.This function is intended to retrieve the number of missing blocks on the receiving end (missing-on-Rx) for a specific type of block (BIB) from a particular source.The function is defined with the name **dtn\_bpsec\_get\_num\_miss\_rx\_bib\_blks\_src** and takes a single argument, a pointer to a **tnvc\_t** structure named parms.

## Supporting Evidence



# 

The above screenshot represents that the error was identified in the code within the “ **adm\_bpsec\_impl.c**”file. The reason for this error to be detected is the second return code that has been added.

# 

# Conclusions and Recommendations

# It's labeled as a "Structurally Dead Code" error, and the message indicates that the code at line 1421 is unreachable. This means that the return result; statement on line 1421 will never be executed because the function already returns a value on line 1415.

The error is just a bug, to resolve this issue, the unreachable return result; statement on line 1421 should be removed.

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.*