**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** |
|  | V0.1 |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

Table of Content

[Introduction 3](#_bookmark0)

[Objective 3](#_bookmark1)

[Scope 3](#_bookmark2)

[Acronyms and Abbreviations 3](#_bookmark3)

[Code Review and Analysis 4](#_bookmark4)

[Outcomes 4](#_bookmark5)

[Observations 4](#_bookmark6)

[Supporting Evidence 4](#_bookmark7)

[Conclusions and Recommendations 4](#_bookmark8)

[References 5](#_bookmark9)

[Appendix 6](#_bookmark10)

# 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

1520785

# 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 |
| BIB | Bundle Integrity block |

# Code Review and Analysis

Overview

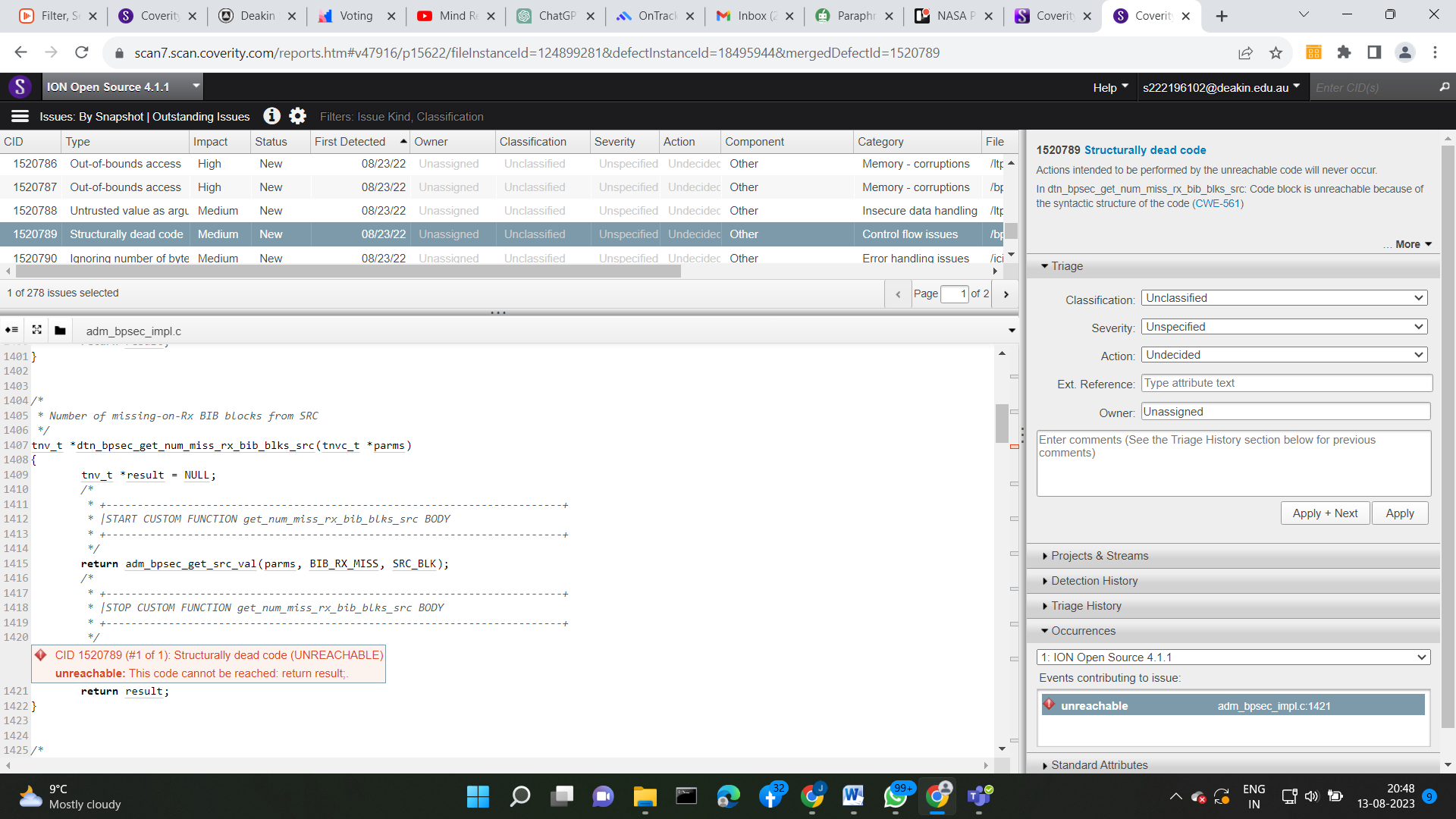
During the analysis of the "adm\_bpsec\_impl.c" codebase within the administration (adm) folder of the Bundle Protocol v7 directory, Coverity has identified instances of "Structurally Dead Code." Specifically, two instances of such dead code have been flagged, one located in the function **dtn\_bpsec\_get\_num\_missing\_rx\_bib\_bytes\_src** (lines 1404-1425) and the other in the function **dtn\_bpsec\_get\_num\_bad\_rx\_bib\_bytes\_src** (lines 1383-1404).

## Observations

* **Functions:**

dtn\_bpsec\_get\_num\_missing\_rx\_bib\_bytes\_src (Lines 1405-1422).

This issue is flagged due to unreachable code within the function **dtn\_bpsec\_get\_num\_missing\_rx\_bib\_bytes\_src**. The core computation is performed by a custom function call at line 1415. However, there is a redundant and unreachable return statement at line 1421. This code segment will never be executed because the preceding return statement at line 1415 terminates the function. As a result, the code at line 1421 is considered structurally dead.

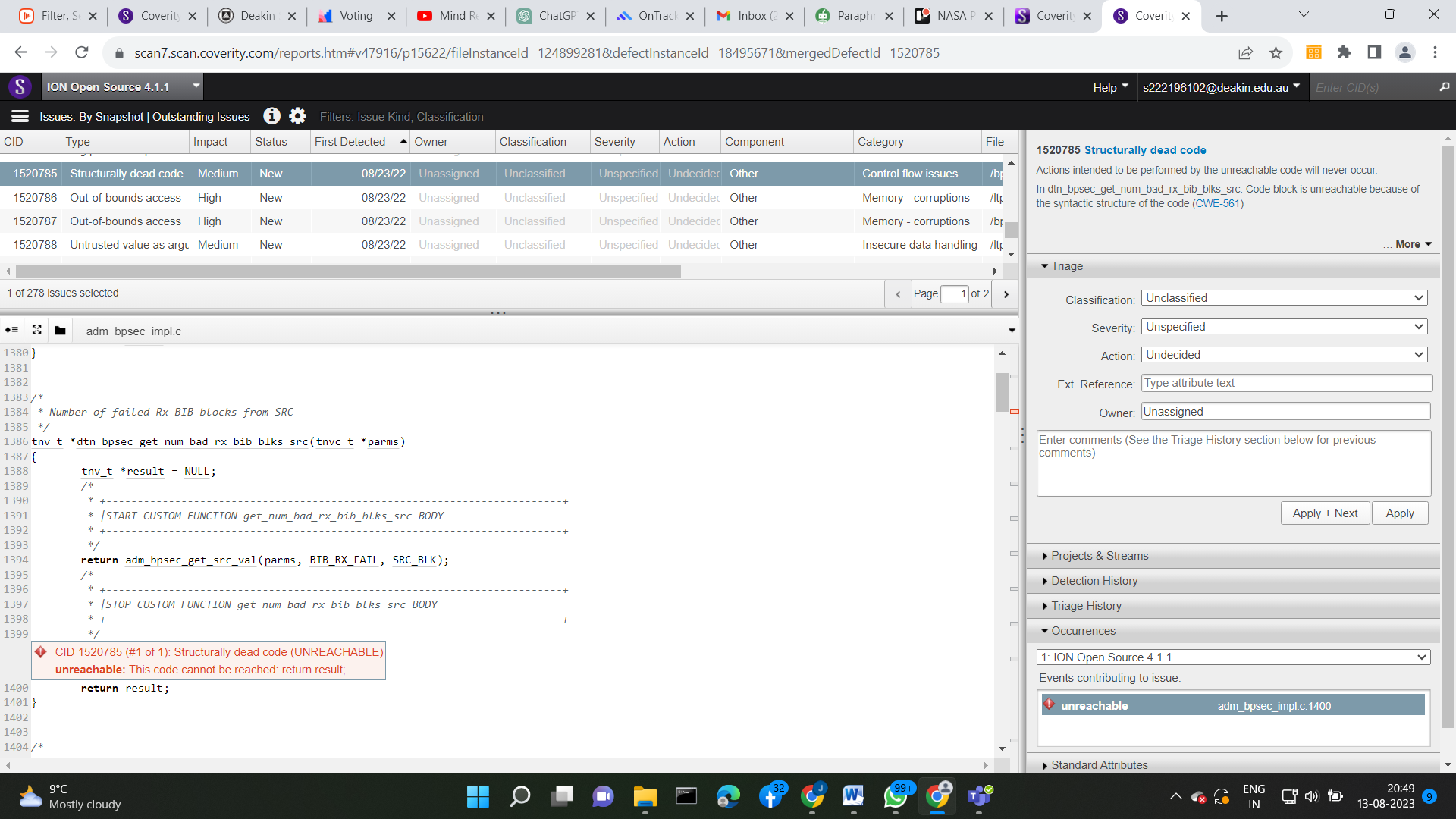


**CID : 1520789**

* **Function:**

dtn\_bpsec\_get\_num\_bad\_rx\_bib\_bytes\_src (Lines 1384-1401)

This issue is similar to the previous one. In the function **dtn\_bpsec\_get\_num\_bad\_rx\_bib\_bytes\_src**, the main computation is executed within a custom function call at line 1389. Subsequently, there is an unreachable return statement at line 1395. This return statement will never be reached due to the earlier return statement at line 1389. Therefore, the code at line 1395 is considered structurally dead.



**CID: 1520785**

## Supporting Evidence

# Conclusions and Recommendations

**Conclusion:**

The presence of "Structurally Dead Code" in the **dtn\_bpsec\_get\_num\_missing\_rx\_bib\_bytes\_src** and **dtn\_bpsec\_get\_num\_bad\_rx\_bIb\_bytes\_src** functions is indicative of unreachable code segments. By eliminating these redundant return statements, the code base will become more concise, comprehensible, and free from the confusion introduced by dead code.

**Recommendations:**

CID 1520785, To resolve this issue, it is advised to remove the unreachable return statement at line 1395, as it does not contribute to the intended functionality of the function.

CID 1520789, To address this issue and improve code readability, it is recommended to remove the redundant and unreachable return statement at line 1421.

# 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.*