**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:

1520805

1520626

# 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 |
| BCB | Bundle Control block |

# Code Review and Analysis

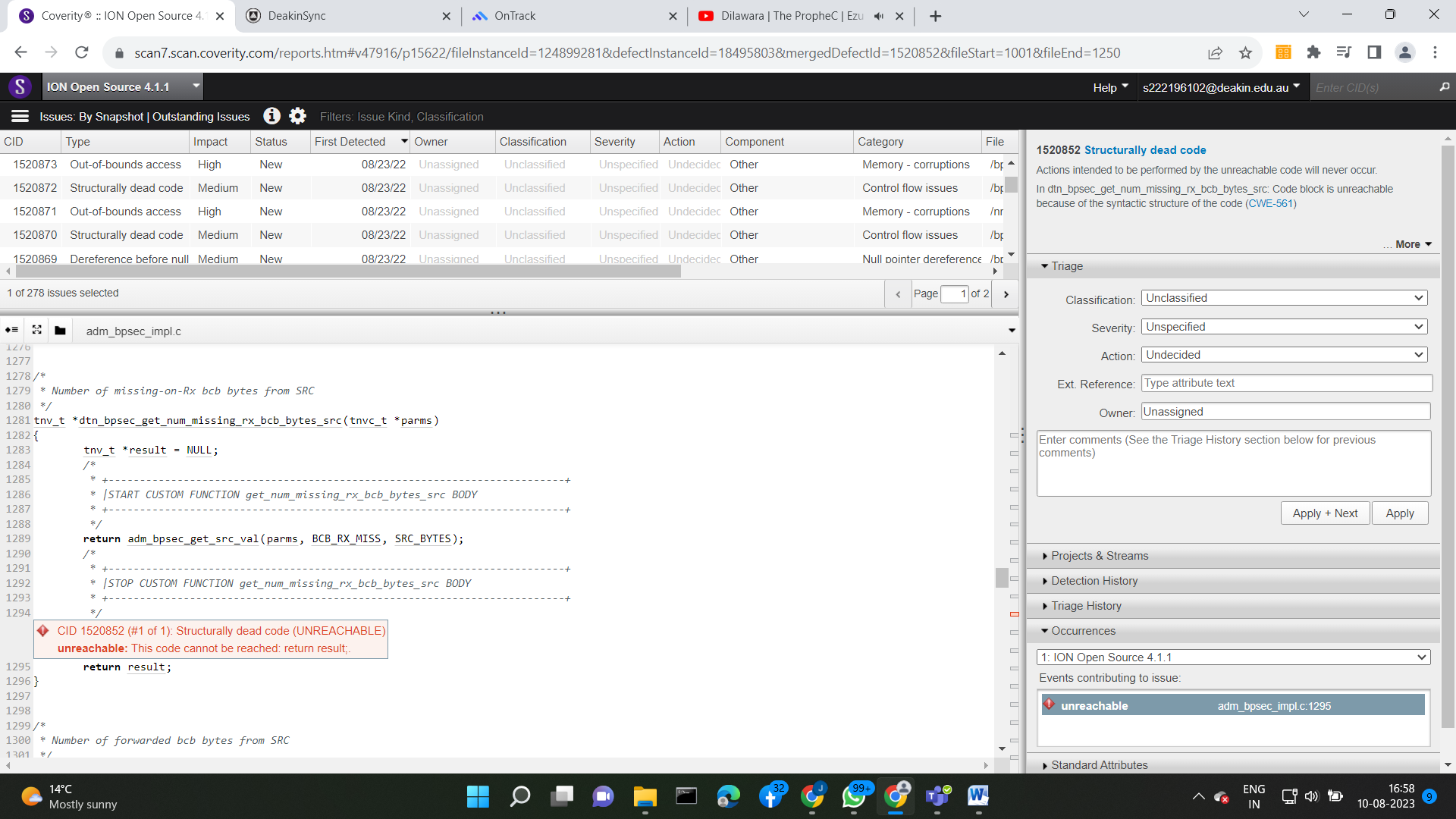
Overview

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\_bcb\_bytes\_src** (lines 1289-1295) and the other in the function **dtn\_bpsec\_get\_num\_bad\_rx\_bcb\_bytes\_src** (lines 1268-1275).

## Observations

An issue has been identified within the **adm\_bpsec\_impl.c** file that pertains to "Structurally Dead Code." This issue is flagged by the Coverity static analysis tool. The dead code is located in two distinct

* **Functions:**

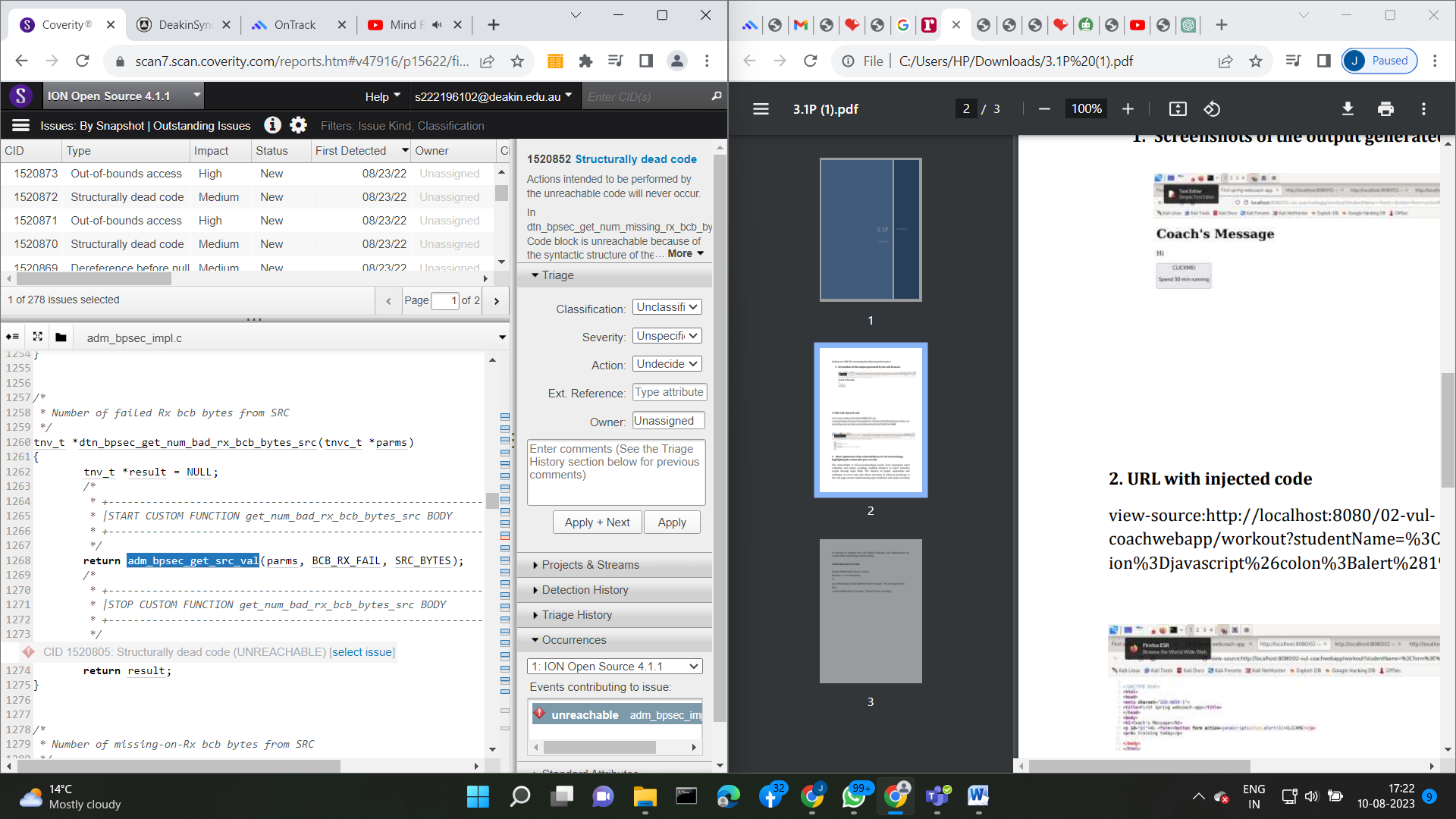
****

**CID : 1520852**

**dtn\_bpsec\_get\_num\_missing\_rx\_bcb\_bytes\_src** and **dtn\_bpsec\_get\_num\_bad\_rx\_bcb\_bytes\_src**.

**Function: dtn\_bpsec\_get\_num\_missing\_rx\_bcb\_bytes\_src (Lines 1282-1296):** In the function **dtn\_bpsec\_get\_num\_missing\_rx\_bcb\_bytes\_src**, the code calculates the number of missing-on-Rx BCB bytes from the source (SRC). The primary functionality is executed within a custom function call at line 1289. The subsequent return statement at line 1295, however, presents an issue. This redundant return statement is never reached due to the earlier return statement. This dead code, marked by CID 1520852, is considered "Structurally Dead Code" since its execution is impossible.

* **Function:**

****

**CID:1520805**

**dtn\_bpsec\_get\_num\_bad\_rx\_bcb\_bytes\_src (Lines 1261-1275):** Similarly, the function **dtn\_bpsec\_get\_num\_bad\_rx\_bcb\_bytes\_src** calculates the number of failed Rx BCB bytes from the source (SRC). The core computation is handled by a custom function call at line 1268. Subsequently, an unreachable return statement at line 1274 follows. As with the previous case, this dead code, identified by CID 1520805, constitutes "Structurally Dead Code" due to its inaccessibility.

## Supporting Evidence

# Conclusions and Recommendations

**Conclusion:**

The presence of "Structurally Dead Code" in the **dtn\_bpsec\_get\_num\_missing\_rx\_bcb\_bytes\_src** and **dtn\_bpsec\_get\_num\_bad\_rx\_bcb\_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:**

To resolve the "Structurally Dead Code" issues and enhance code readability, it is recommended to remove the redundant and unreachable return statements. These lines of code do not contribute to the intended functionality of the functions and only add unnecessary complexity.

# 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.*