**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** |
| 1/08/23 | V0.1 | John-Eddie Cubis | Analysis of Structurally dead code. |
|  |  |  |  |
|  |  |  |  |

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 4](#_Toc119848732)

[References 5](#_Toc119848733)

[Appendix 6](#_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 ***Structurally dead code*** type defect identified in the following CIDs:  
***1520828***[***, Dead Code***](https://cwe.mitre.org/data/definitions/561.html)

***1520867,*** [***Dead Code***](https://cwe.mitre.org/data/definitions/561.html)

***1520762,*** [***Dead Code***](https://cwe.mitre.org/data/definitions/561.html)

# 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 |

# Code Review and Analysis

## Overview

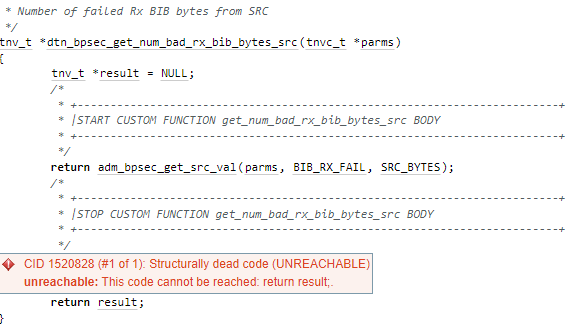
The Coverity Static Analysis tool identified several Structurally dead pieces of code within the Bundle Protocol v7 extensions within the [/bpv7/adm/adm\_bpsec\_impl.c] path. The following covers observation, risks and mitigation methods when dealing with structurally dead code.

## Observations

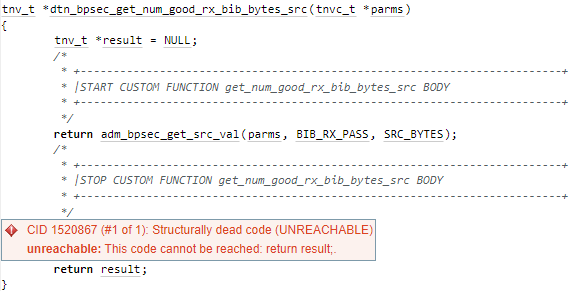
CWE (Common Weakness Enumeration) states, dead code is deemed unsafe and increases the chance of an exploitable vulnerability present in a application, while these may not directly induce a vulnerability, however may indicate best practice has not been implemented or maintained.

Below are the following CIDs in this report:

**1520828:**



**1520867:**

****

**1520762:**

**A screenshot of a computer code

Description automatically generated**

These functions within the ION Open source check the number of failed, successful BIB bytes in SRC, and returns the statement adm\_bpsec\_get\_src\_val. After this statement there is another return result that is unreachable, the call return before this second return function **(return result;)** executes. Any code after will not be used, therefore is detected as structurally dead code.

## Supporting Evidence

Please provide any supporting evidence, and feel free to make references to documents in the appendix.

# Conclusions and Recommendations

To fix this issue for the following CID’s is to remove the ‘return result;’ statement.

**tnv\_t \*dtn\_bpsec\_get\_num\_good\_rx\_bib\_bytes\_src(tnvc\_t \*parms)**

**{**

**tnv\_t \*result = NULL;**

**/\***

**\* +-------------------------------------------------------------------------+**

**\* |START CUSTOM FUNCTION get\_num\_good\_rx\_bib\_bytes\_src BODY**

**\* +-------------------------------------------------------------------------+**

**\*/**

**return adm\_bpsec\_get\_src\_val(parms, BIB\_RX\_PASS, SRC\_BYTES);**

**/\***

**\* +-------------------------------------------------------------------------+**

**\* |STOP CUSTOM FUNCTION get\_num\_good\_rx\_bib\_bytes\_src BODY**

**\* +-------------------------------------------------------------------------+**

**\*/**

**}**

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.