**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** |
| 04/08/2023 | V1.0 | Adharshaan Devaraj | Initial Document |
|  |  |  |  |
|  |  |  |  |

Table of Content

Contents

[Introduction 3](#_Toc133624419)

[Objective 3](#_Toc133624420)

[Scope 3](#_Toc133624421)

[Acronyms and Abbreviations 3](#_Toc133624422)

[Code Review and Analysis 4](#_Toc133624423)

[Overview 4](#_Toc133624424)

[Observations 4](#_Toc133624425)

[Supporting Evidence 4](#_Toc133624426)

[Conclusions and Recommendations 4](#_Toc133624427)

[References 5](#_Toc133624428)

[Appendix 5](#_Toc133624429)

# 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:  
***1520631***

***1520635***

# 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 |
| BCB | Bundle Confidentiality Block |

# Code Review and Analysis

## Overview

By analyzing “**adm\_bpsec\_impl.c”** code base within the **administration (adm)** folder of the Bundle Protocol v7 directory. Coverity highlighted a “**Structurally Dead Code”** error that highlights the use of dead code that cannot be executed at line 1211 in CID 1520631 and 1358 in CID 1520635. The **tnv\_t \*dtn\_bpsec\_get\_num\_good\_tx\_bcb\_bytes\_src(tnvc\_t \*parms)** and **tnv\_t \*dtn\_bpsec\_get\_num\_ bad\_tx\_bib\_blks\_src(tnvc\_t \*parms)** functions which outputs the successfully transmitted number of bytes and the count of bad BIB blocks.

## Observations

The "**adm\_bpsec\_impl.c**" file implements functions from the BPSEC Administration API in ION, which provides the setting and administration of security policies and bundle information. The function **tnv\_t \*dtn\_bpsec\_get\_num\_good\_tx\_bcb\_bytes\_src(tnvc\_t \*parms)** is used to find the number of bytes that were successfully transmitted as part of the BCB.

The function in CID 1520631 seems to be designed to provide information about the number of bytes that were successfully transmitted as part of the BCB during the secure communication process from the source node. It may be used for monitoring and evaluation of security-related metrics in a DTN network that utilizes BPSEC for secure bundle transmissions.

The function, **tnv\_t \*dtn\_bpsec\_get\_num\_ bad\_tx\_bib\_blks\_src(tnvc\_t \*parms)** in CID 1520635 is used to retrieve the number of bad (corrupted or invalid) BIB blocks for a particular source. The function probably performs some analysis on the BPsec-related data structures to determine the count of bad BIB blocks.

The error was detected because a second return code has been written in the function. This second return code cannot be executed because another return code has been written before that hence this error is being detected. The second return code cannot be executed because the first code would have run before this hence the structurally dead code is being detected.

## Supporting Evidence

A screenshot of a computer code

Description automatically generated

Figure - CID 1520631

The above screenshot represents the error that 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 to the code. (CWE, 2006)

A screenshot of a computer code

Description automatically generated

Figure - CID 1520791

The above screenshot represents the error that 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 to the code. (CWE, 2006)

# Conclusions and Recommendations

This error is just a bug in the code hence to resolve this error the second return code must be removed from the function.

# References

CWE, 2006. *CWE-561: Dead Code.* [Online]   
Available at: https://cwe.mitre.org/data/definitions/561.html  
[Accessed 2023].

Appendix

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