Coverity Scan Vulnerability Assessment Report

Hardhard Enterprises

**T3** 2022

Statement of Intent

Overview

This document aims to provide a record of the vulnerability assessment performed on a specific issue from the Coverity SAST scan for the NASA ION Open-Source code 4.1.1 project and is a follow-up report from the static analysis report.

The primary purpose of this document is to provide an in-depth assessment of the identified vulnerability. Assessment includes but is not limited to; Recreating the issue, investigating the potential for exploitation, deploying various exploits and reporting on the researcher's findings.

Depending on findings, secondary purposes can include but are not limited to listing/providing recommended fixes alongside a list of potential attack vectors/scenarios.

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. Adhering to these practices will better inform readers and 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 the Microsoft Word 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; VAR\_{CID}. For example, when investigating issue 123456, the file name would be VAR\_123456.docx

Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Dates** | **Version** | **Author** | **Comments** |
| 6/12/2022 | V1.0 | Tristen Clifton | Itital document |
|  |  |  |  |
|  |  |  |  |

Table of Content

Contents

[Introduction 3](#_Toc119932107)

[Objective 3](#_Toc119932108)

[Scope 3](#_Toc119932109)

[Acronyms and Abbreviations 3](#_Toc119932110)

[Vulnerability Assessment Report 4](#_Toc119932111)

[Recreating the Issue 4](#_Toc119932112)

[Overview 4](#_Toc119932113)

[Finding and Observations 4](#_Toc119932114)

[Exploiting the Issue 4](#_Toc119932115)

[Overview 4](#_Toc119932116)

[Finding and Observations 4](#_Toc119932117)

[Supporting Evidence 4](#_Toc119932118)

[Recommendation(s) to fix. 4](#_Toc119932119)

[Conclusions and Recommendations 4](#_Toc119932120)

[References 5](#_Toc119932121)

[Appendix 6](#_Toc119932122)

# Introduction

## Objective

The primary objective of this assessment is to determine whether the defects identified in the Coverity Report for the ION Open Source 4.1.1 project are:

* Indeed, recreatable.
* Indeed, exploitable.

The secondary objective of this analysis, where applicable, is to provide the following:

* Comprehensive details on the exploit itself.
* Any additional exploitable scenarios.
* A detailed list of attack vectors.
* Recommendation(s) to fix.

## Scope

This vulnerability assessment is limited to the ***String not null terminated*** type defect identified in the following CIDs:  
***1520742***

# Acronyms and Abbreviations

Please keep an updated list of acronyms and abbreviations used throughout the report.

|  |  |
| --- | --- |
| **Acronym / Abbr.** | **Meaning** |
| DTN | Delay/Disruption Tolerant Network |
| ION | Interplanetary Overlay Network |
| CID | Coverity Issue Identification Number |

# Vulnerability Assessment Report

## Recreating the Issue

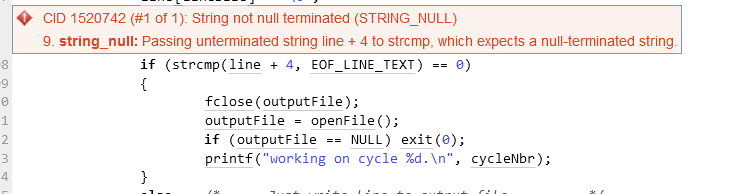
### Overview

A string\_null is a vulnerability that exists when a string varible has been created without assigning a null terminator to the end of the string. This pointer would normally be used to indicate to the program that it has reached the end of the array (the string of characters). Without it the string could potentially cause the program to have unexpected looping or overflow effects.

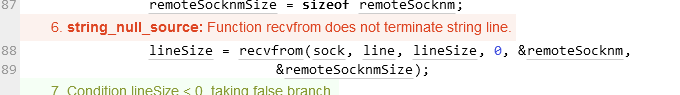
This could also be labled as a security risk as a string without null termination could could lead to a buffer overflow condiction would could be exploited to execute arbitrary code.

### Finding and Observations

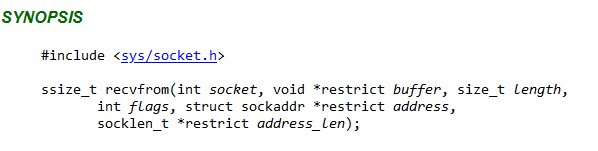
The Coverity scan reported the issue when it noticed that the varible “line” (what it assumed to be a non-null terminated value) was used as an input into the function strcmp.



Looking further into the code we can see that the origin source is the function recvfrom that apparently manipulates the value, resulting in the problematic varible.



For the issue to be no longer be detected by the scan and to fix the issue we would need to modify the function recvfrom to null terminate the string when called. However this is not possible as the function comes from a standard library and should not be modified

‘

However, when we dug further into the code, we observed that a method was already present to null terminate the string.



This line assigned a null pointer to the end of the array ensuring it was null terminated.

Because this was done after the function call it was not recognised by the system but resolved the vulnerability. From this information we can assign this detection as a false positive.

# Conclusions and Recommendations

In conclusion, a risk was rightfully detected by the system, however the countermeasure that was already in place was not, thefore the risk was non existent meaning that this CID can be marked as a false positive

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).

cwe.mitre.org. (n.d.). *CWE - CWE-170: Improper Null Termination (4.9)*. [online] Available at: https://cwe.mitre.org/data/definitions/170.html [Accessed 6 Dec. 2022].

‌scan7.scan.coverity.com. (n.d.). *Coverity® :: Sign in*. [online] Available at: https://scan7.scan.coverity.com/doc/en/cov\_checker\_ref.html#static\_checker\_STRING\_NULL [Accessed 6 Dec. 2022].

‌pubs.opengroup.org. (n.d.). *recvfrom*. [online] Available at: https://pubs.opengroup.org/onlinepubs/007904875/functions/recvfrom.html [Accessed 6 Dec. 2022].

‌

Appendix

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