Polyspace Bug Finder

Polyspace CWE Report for Project: cwe

Report Author: YangLiMin

Polyspace Bug Finder: Polyspace CWE Report for Project: cwe

by Report Author: YangLiMin

Published 02-Dec-2024 14:11:30

Analysis Author(s): YangLiMin  
Polyspace Version(s): Polyspace Bug Finder 3.2 (R2020a)  
Project Version(s): 1.0  
  
  
  
  
  
  
Result Folder(s):  
C:\Users\yanglimin\Documents\Polyspace\_Workspace\Module\_1\BF\_Result\_5

Table of Contents

[Chapter 1. Polyspace Bug Finder Summary 1](#_Toc184041130)

[Chapter 2. Defects 8](#_Toc184041131)

[**Defects** 8](#_Toc184041132)

[Chapter 3. Appendix 1 - Configuration Settings 36](#_Toc184041133)

[**Polyspace Settings** 36](#_Toc184041134)

[**Security Standard to Polyspace Result Map** 37](#_Toc184041135)

[**Files with compilation errors (files partially analyzed)** 54](#_Toc184041136)

[Chapter 4. Appendix 2 - Definitions 56](#_Toc184041137)

Chapter 1. Polyspace Bug Finder Summary

Table 1.1. Project Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Count** | **Reviewed** | **Unreviewed** | **Pass/Fail** |
| Defects | 167 | 0 | 167 | NA |
| **Total** | **167** | **0** | **167** | **NA** |

Table 1.2. Summary By File

|  |  |
| --- | --- |
| **File** | **Defects (Reviewed)** |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_119.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_119.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_120.c | 3 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_120.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_121.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_121.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_122.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_122.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_124.c | 6 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_124.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_125.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_125.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_126.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_126.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_129.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_129.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_130.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_130.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_131.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_131.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_1335.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_1335.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_134.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_134.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_170.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_170.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_176.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_176.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_188.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_188.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_190.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_190.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_191.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_191.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_192.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_192.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_193.c | 3 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_193.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_194.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_194.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_195.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_195.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_196.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_196.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_197.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_197.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_20.c | 6 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_20.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_234.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_234.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_242.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_242.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_252.c | 3 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_252.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_253.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_253.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_369.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_369.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_391.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_391.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_393.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_393.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_400.c | 5 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_400.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_401.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_401.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_404.c | 6 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_404.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_415.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_415.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_416.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_416.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_456.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_456.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_457.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_457.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_459.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_459.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_467.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_467.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_468.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_468.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_469.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_469.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_476.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_476.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_478.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_478.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_480.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_480.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_481.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_481.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_482.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_482.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_483.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_483.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_484.c | 11 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_484.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_561.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_561.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_562.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_562.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_563.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_563.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_570.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_570.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_571.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_571.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_587.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_587.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_588.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_588.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_590.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_590.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_605.c | 4 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_605.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_606.c | 3 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_606.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_665.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_665.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_670.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_670.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_672.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_672.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_674.c | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_674.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_676.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_676.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_680.c | 3 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_680.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_681.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_681.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_682.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_682.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_685.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_685.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_686.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_686.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_688.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_688.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_690.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_690.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_704.c | 5 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_704.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_761.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_761.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_787.c | 6 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_787.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_788.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_788.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_789.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_789.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_805.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_805.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_806.c | 3 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_806.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_824.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_824.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_835.c | 2 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_835.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_843.c | 1 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_843.h | 0 (0) |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\MAIN.c | 0 (0) |

Table 1.3. Files with compilation errors (files partially analyzed)

|  |
| --- |
| **File** |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_134.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_176.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_469.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_483.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_561.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_588.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_670.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_672.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\MAIN.c |

Chapter 2. Defects

Defects

Table 2.1. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_119.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 53 | Tainted NULL or non-null-terminated string | Low | copy\_input() | Argument to 'strlen' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |
| 54 | Use of tainted pointer | Low | copy\_input() | Dereferenced pointer is from an unsecure source. Pointer may be NULL or may point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |

Table 2.2. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_120.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 3 | Hard-coded buffer size | Low | test\_cwe\_120() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 55 | Returned value of a sensitive function not checked | High | test\_cwe\_120() | Return value of 'scanf' not checked. 'scanf' returns items to the argument list on success, possibly fewer than expected, or EOF on failure. To ignore this defect, cast 'scanf' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 2 | Buffer overflow from incorrect string format specifier | High | test\_cwe\_120() | Format specifier '%s' causes overflow in string buffer of 20 characters. | Unset | Unreviewed |  | CWE-124 CWE-125 CWE-126 CWE-127 |

Table 2.3. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_121.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 1 | Hard-coded buffer size | Low | CWE\_121\_BufferOverflow() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 56 | Tainted NULL or non-null-terminated string | Low | CWE\_121\_BufferOverflow() | Second argument to 'strcpy' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |

Table 2.4. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_122.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 58 | Invalid use of standard library string routine | High | CWE\_122\_HeapBufferOverflow() | Standard function 'strcpy' may be called with an invalid argument.  first argument (destination) may not be the correct size. | Unset | Unreviewed |  | CWE-120 CWE-227 CWE-690 |
| 57 | Tainted NULL or non-null-terminated string | Low | CWE\_122\_HeapBufferOverflow() | Second argument to 'strcpy' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |

Table 2.5. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_124.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 59 | Memory allocation with tainted size | Medium | CWE\_124\_TrimTrailingWhitespace() | Memory may be allocated with tainted size. Call to function malloc | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-789 |
| 60 | Tainted sign change conversion | Medium | CWE\_124\_TrimTrailingWhitespace() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |
| 62 | Loop bounded with tainted value | Medium | CWE\_124\_TrimTrailingWhitespace() | Loop is controlled by a value from an unsecure source. Loop may be infinite. | Unset | Unreviewed |  | CWE-606 |
| 61 | Use of tainted pointer | Low | CWE\_124\_TrimTrailingWhitespace() | Dereferenced pointer is from an unsecure source. Pointer may be NULL or may point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |
| 63 | Misuse of sign-extended character value | Medium | CWE\_124\_TrimTrailingWhitespace() | 'isspace' argument has undergone conversions with sign extension and can be out of expected range [0..UCHAR\_MAX]. 'isspace' can cause unexpected result. To fix, cast the character value to 'unsigned char' before conversion to a wider type. | Unset | Unreviewed |  | CWE-704 |
| 64 | Pointer access out of bounds | High | CWE\_124\_TrimTrailingWhitespace() | Pointer points to a memory block of [1 .. ?] bytes. | Unset | Unreviewed |  | CWE-119 CWE-131 CWE-188 CWE-466 CWE-823 |

Table 2.6. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_125.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 67 | Use of tainted pointer | Low | CWE\_125\_GetValueFromArray() | Dereferenced pointer is from an unsecure source. Pointer may be NULL or may point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |
| 68 | Pointer dereference with tainted offset | Low | CWE\_125\_GetValueFromArray() | Offset used to dereference pointed object is from an unsecure source. Dereference may be out of bounds. | Unset | Unreviewed |  | CWE-122 CWE-124 CWE-129 CWE-823 |
| 65 | Use of tainted pointer | Low | CWE\_125\_GetValueFromArray() | Dereferenced pointer is from an unsecure source. Pointer may be NULL or may point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |
| 66 | Pointer dereference with tainted offset | Low | CWE\_125\_GetValueFromArray() | Offset used to dereference pointed object is from an unsecure source. Dereference may be out of bounds. | Unset | Unreviewed |  | CWE-122 CWE-124 CWE-129 CWE-823 |

Table 2.7. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_126.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 160 | Invalid use of standard library memory routine | High | getMessage() | Standard function 'memset' is called with an invalid argument.  # Checks on first argument (destination):  Is not a memory area that is accessible within the boundary given by the third argument. | Unset | Unreviewed |  | CWE-120 CWE-227 CWE-690 |
| 69 | Tainted sign change conversion | Medium | getMessage() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |
| 161 | Array access out of bounds | High | CWE\_126\_ProcessMessageFromSocket() | Attempt to access to array element in range [128 .. 255].  Valid index range: [0 .. 127]. | Unset | Unreviewed |  | CWE-119 CWE-131 CWE-466 |
| 162 | Array access out of bounds | High | CWE\_126\_ProcessMessageFromSocket() | Attempt to access to array element 256.  Valid index range: [0 .. 127]. | Unset | Unreviewed |  | CWE-119 CWE-131 CWE-466 |

Table 2.8. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_129.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 70 | Use of tainted pointer | Low | CWE\_129\_GetValueFromIndex() | Dereferenced pointer is from an unsecure source. Pointer may be NULL or may point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |
| 71 | Pointer dereference with tainted offset | Low | CWE\_129\_GetValueFromIndex() | Offset used to dereference pointed object is from an unsecure source. Dereference may be out of bounds. | Unset | Unreviewed |  | CWE-122 CWE-124 CWE-129 CWE-823 |

Table 2.9. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_130.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 165 | Invalid use of standard library memory routine | High | getMessage() | Standard function 'memset' is called with an invalid argument.  # Checks on first argument (destination):  Is not a memory area that is accessible within the boundary given by the third argument. | Unset | Unreviewed |  | CWE-120 CWE-227 CWE-690 |
| 72 | Tainted sign change conversion | Medium | getMessage() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |
| 163 | Array access out of bounds | High | CWE\_130\_ProcessMessageFromSocket() | Attempt to access to array element in range [128 .. 255].  Valid index range: [0 .. 127]. | Unset | Unreviewed |  | CWE-119 CWE-131 CWE-466 |
| 164 | Array access out of bounds | High | CWE\_130\_ProcessMessageFromSocket() | Attempt to access to array element 256.  Valid index range: [0 .. 127]. | Unset | Unreviewed |  | CWE-119 CWE-131 CWE-466 |

Table 2.10. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_131.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 73 | Tainted NULL or non-null-terminated string | Low | CWE\_131\_CopyInput() | Argument to 'strlen' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |
| 74 | Use of tainted pointer | Low | CWE\_131\_CopyInput() | Dereferenced pointer is from an unsecure source. Pointer may be NULL or may point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |

Table 2.11. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_170.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 4 | Hard-coded buffer size | Low | CWE170\_ImproperNullTermination() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |

Table 2.12. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_188.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 75 | Write without a further read | Low | CWE188\_RelianceOnDataMemoryLayout() | Variable 'pchar' is never read after this point. | Unset | Unreviewed |  | CWE-398 |

Table 2.13. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_190.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 76 | Memory allocation with tainted size | Medium | CWE\_190\_AllocateImageTable() | Memory may be allocated with tainted size. Call to function malloc | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-789 |
| 77 | Tainted sign change conversion | Medium | CWE\_190\_AllocateImageTable() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |

Table 2.14. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_191.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 79 | Write without a further read | Low | CWE\_191\_IntegerUnderflow() | Variable 'i' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 78 | Integer overflow | Medium | CWE\_191\_IntegerUnderflow() | Operation - overflows. Valid range: [-2^31 .. 2^31-1] | Unset | Unreviewed |  | CWE-128 CWE-189 CWE-190 CWE-191 CWE-192 |

Table 2.15. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_192.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 5 | Hard-coded buffer size | Low | GetUserInput() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 6 | Hard-coded buffer size | Low | CWE\_192\_IntegerCastingError() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 166 | Integer conversion overflow | High | CWE\_192\_IntegerCastingError() | Conversion from int32 to int16 overflows. Valid range: [-32768 .. 32767] | Unset | Unreviewed |  | CWE-128 CWE-189 CWE-190 CWE-191 CWE-192 CWE-197 |
| 167 | Tainted sign change conversion | Medium | CWE\_192\_IntegerCastingError() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |

Table 2.16. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_193.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 7 | Hard-coded buffer size | Low | CWE\_193\_OffByOneError() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 81 | Tainted NULL or non-null-terminated string | Low | CWE\_193\_OffByOneError() | Second argument to 'strncat' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |
| 82 | Tainted NULL or non-null-terminated string | Low | CWE\_193\_OffByOneError() | Second argument to 'strncat' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |

Table 2.17. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_194.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 8 | Hard-coded buffer size | Low | GetUserInput() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 9 | Hard-coded buffer size | Low | CWE\_194\_UnexpectedSignExtension() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 168 | Integer conversion overflow | High | CWE\_194\_UnexpectedSignExtension() | Conversion from int32 to int16 overflows. Valid range: [-32768 .. 32767] | Unset | Unreviewed |  | CWE-128 CWE-189 CWE-190 CWE-191 CWE-192 CWE-197 |
| 169 | Tainted sign change conversion | Medium | CWE\_194\_UnexpectedSignExtension() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |

Table 2.18. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_195.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 84 | Sign change integer conversion overflow | Medium | CWE\_195\_SignedToUnsignedConversionError() | Conversion from int32 to unsigned int32 overflows. Valid range: [0 .. 2^32-1] | Unset | Unreviewed |  | CWE-192 CWE-194 CWE-195 CWE-196 |

Table 2.19. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_196.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 86 | Write without a further read | Low | CWE\_196\_SignConversionError() | Variable 'ret' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 85 | Sign change integer conversion overflow | Medium | CWE\_196\_SignConversionError() | Conversion from unsigned int8 to int8 overflows. Valid range: [-128 .. 127] | Unset | Unreviewed |  | CWE-192 CWE-194 CWE-195 CWE-196 |

Table 2.20. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_197.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 89 | Bitwise operation on negative value | Medium | CWE\_197\_NumericTruncationError() | Left operand of ^ is negative. A ^ operation on negative value may alter the sign bit and lead to the result misinterpretation. Use unsigned integer type or avoid negative values. | Unset | Unreviewed |  | CWE-682 CWE-758 |
| 87 | Integer overflow | Medium | CWE\_197\_NumericTruncationError() | Operation << overflows. Valid range: [-2^31 .. 2^31-1] | Unset | Unreviewed |  | CWE-128 CWE-189 CWE-190 CWE-191 CWE-192 |
| 88 | Integer precision exceeded | Low | CWE\_197\_NumericTruncationError() | Shift count (right operand) of << is computed from sizeof(). Shift count may exceed precision of result type, and shift operation may result in unexpected value. To fix, use a shift count smaller than the precision of result type. | Unset | Unreviewed |  | CWE-190 |
| 10 | Integer constant overflow | Medium | CWE\_197\_NumericTruncationError() | Overflow on signed constant | Unset | Unreviewed |  | CWE-128 CWE-189 CWE-190 CWE-191 |

Table 2.21. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_20.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 91 | Unsafe conversion from string to numerical value | Low | CWE20\_ImproperInputValidation() | Converted value may be incorrect without additional checks. 'scanf' cannot report errors for invalid integer values associated with the conversion specifier #1. Use 'strtol', 'strtoll', 'strtoul', 'strtoull' or a related function with more robust error handling. | Unset | Unreviewed |  | CWE-20 CWE-253 CWE-676 |
| 92 | Unsafe conversion from string to numerical value | Low | CWE20\_ImproperInputValidation() | Converted value may be incorrect without additional checks. 'scanf' cannot report errors for invalid integer values associated with the conversion specifier #1. Use 'strtol', 'strtoll', 'strtoul', 'strtoull' or a related function with more robust error handling. | Unset | Unreviewed |  | CWE-20 CWE-253 CWE-676 |
| 95 | Write without a further read | Low | CWE20\_ImproperInputValidation() | Variable 'board' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 93 | Memory allocation with tainted size | Medium | CWE20\_ImproperInputValidation() | Memory may be allocated with tainted size. Call to function malloc | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-789 |
| 94 | Tainted sign change conversion | Medium | CWE20\_ImproperInputValidation() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |
| 90 | Memory leak | Medium | CWE20\_ImproperInputValidation() | Pointer 'board' points to dynamically allocated memory. It has not been freed before the end of its scope. | Unset | Unreviewed |  | CWE-401 CWE-404 |

Table 2.22. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_242.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 97 | Returned value of a sensitive function not checked | High | CWE\_242\_UseOfDangerousFunction() | Return value of 'gets' not checked. 'gets' returns the pointer of the first argument on success, NULL on end-of-file or failure. To ignore this defect, cast 'gets' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 96 | Use of dangerous standard function | Low | CWE\_242\_UseOfDangerousFunction() | Using 'gets' can cause the destination buffer to overflow. 'gets' cannot control the length of input from the console. Use 'fgets(dest, size, stdin)' instead. | Unset | Unreviewed |  | CWE-242 CWE-676 |

Table 2.23. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_252.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 11 | Hard-coded buffer size | Low | CWE\_252\_UncheckedReturnValue() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 12 | Hard-coded buffer size | Low | CWE\_252\_UncheckedReturnValue() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 98 | Returned value of a sensitive function not checked | High | CWE\_252\_UncheckedReturnValue() | Return value of 'fgets' not checked. 'fgets' returns the pointer of the first argument on success, NULL on end-of-file or failure. To ignore this defect, cast 'fgets' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |

Table 2.24. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_253.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 46 | Memory leak | Medium | CWE\_253\_IncorrectCheckOfReturnValue() | Pointer 'tmp' points to dynamically allocated memory. It has not been freed before the end of its scope. | Unset | Unreviewed |  | CWE-401 CWE-404 |

Table 2.25. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_369.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 99 | Tainted division operand | Low | CWE\_369\_ComputeAverageResponseTime() | Division (/) operation operands are from an unsecure source. Check for: - Denominator of zero. - Numerator of minimum value and denominator of -1. | Unset | Unreviewed |  | CWE-189 CWE-190 CWE-369 |

Table 2.26. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_391.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 13 | Hard-coded buffer size | Low | CWE\_391\_UncheckedErrorCondition() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |

Table 2.27. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_400.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 104 | Returned value of a sensitive function not checked | High | CWE\_400\_UncontrolledResourceConsumption() | Return value of 'close' not checked. 'close' returns 0 on success or -1 on failure. To ignore this defect, cast 'close' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 102 | Returned value of a sensitive function not checked | High | CWE\_400\_UncontrolledResourceConsumption() | Return value of 'close' not checked. 'close' returns 0 on success or -1 on failure. To ignore this defect, cast 'close' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 101 | Standard function call with incorrect arguments | Medium | CWE\_400\_UncontrolledResourceConsumption() | File associated with 'close' closed earlier. | Unset | Unreviewed |  | CWE-628 CWE-685 CWE-686 CWE-687 CWE-690 CWE-910 |
| 103 | Returned value of a sensitive function not checked | High | CWE\_400\_UncontrolledResourceConsumption() | Return value of 'close' not checked. 'close' returns 0 on success or -1 on failure. To ignore this defect, cast 'close' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 100 | Returned value of a sensitive function not checked | High | CWE\_400\_UncontrolledResourceConsumption() | Return value of 'close' not checked. 'close' returns 0 on success or -1 on failure. To ignore this defect, cast 'close' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |

Table 2.28. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_401.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 47 | Memory leak | Medium | CWE\_401\_GetBlock() | Pointer 'buf' points to dynamically allocated memory. It has not been freed before the end of its scope. | Unset | Unreviewed |  | CWE-401 CWE-404 |

Table 2.29. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_404.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 171 | Inappropriate I/O operation on device files | Medium | CWE\_404\_DecodeFile() | 'fopen' is appropriate only for regular files but the file argument could be a device or its symbolic link. To fix, you can \* Check the argument for a regular file (using 'stat', 'lstat' or equivalent). \* Compare the argument against a list of devices name as black list. | Unset | Unreviewed |  | CWE-67 |
| 107 | Vulnerable path manipulation | Low | CWE\_404\_DecodeFile() | Path argument to 'fopen' may contain '..', '/abs/path/', or other unsecure elements. | Unset | Unreviewed |  | CWE-22 CWE-23 CWE-36 |
| 106 | Tainted NULL or non-null-terminated string | Low | CWE\_404\_DecodeFile() | First argument to 'fopen' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |
| 172 | Dead code | Low | CWE\_404\_DecodeFile() | If-condition always evaluates to false. Dead branch from line 25 to line 28. | Unset | Unreviewed |  | CWE-561 |
| 170 | Resource leak | High | CWE\_404\_DecodeFile() | Stream 'f' has not been closed before the end of its scope. | Unset | Unreviewed |  | CWE-772 |
| 173 | Returned value of a sensitive function not checked | High | CWE\_404\_DecodeFile() | Return value of 'fclose' not checked. 'fclose' returns zero on success or EOF on failure. To ignore this defect, cast 'fclose' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |

Table 2.30. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_415.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 14 | Missing reset of freed pointer | Low | CWE\_415\_DoubleFree() | After free(), local variable 'ptr' still holds an address accessible from the local scope. To prevent dangling pointers, after calling free(), immediately set the pointer to NULL. | Unset | Unreviewed |  | CWE-415 CWE-416 CWE-825 |
| 109 | Deallocation of previously deallocated pointer | High | CWE\_415\_DoubleFree() | Pointer may be already deallocated. | Unset | Unreviewed |  | CWE-415 CWE-825 |

Table 2.31. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_416.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 15 | Missing reset of freed pointer | Low | CWE\_416\_UseAfterFree() | After free(), local variable 'ptr' still holds an address accessible from the local scope. To prevent dangling pointers, after calling free(), immediately set the pointer to NULL. | Unset | Unreviewed |  | CWE-415 CWE-416 CWE-825 |
| 49 | Memory leak | Medium | CWE\_416\_UseAfterFree() | Pointer 'ptr' points to dynamically allocated memory. It has not been freed before the end of its scope. | Unset | Unreviewed |  | CWE-401 CWE-404 |

Table 2.32. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_456.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 110 | Tainted NULL or non-null-terminated string | Low | CWE\_456\_ParseData() | First argument to 'sscanf' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |

Table 2.33. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_457.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 111 | Non-initialized pointer | High | CWE\_457\_UseOfUninitializedVariable() | Local pointer 'test\_string' may be read before being initialized. | Unset | Unreviewed |  | CWE-456 CWE-457 CWE-824 CWE-908 |

Table 2.34. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_459.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 113 | Returned value of a sensitive function not checked | High | MKSTEMP() | A sensitive function returns error or state information. Check the return value before using it. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 112 | Returned value of a sensitive function not checked | High | CWE\_459\_IncompleteCleanup() | Return value of 'fclose' not checked. 'fclose' returns zero on success or EOF on failure. To ignore this defect, cast 'fclose' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |

Table 2.35. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_467.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 116 | Write without a further read | Low | CWE\_467\_UseOfSizeofOnPointerType() | Variable 'foo' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 115 | Wrong allocated object size for cast | High | CWE\_467\_UseOfSizeofOnPointerType() | The size of the allocated memory is not a multiple of the destination pointer size. Allocated memory: 4 bytes Destination size: 8 bytes (float 64) | Unset | Unreviewed |  | CWE-704 |
| 16 | Wrong type used in sizeof | High | CWE\_467\_UseOfSizeofOnPointerType() | The type 'double \*' used for the block of memory is not a pointer to the type 'double \*' used in sizeof. | Unset | Unreviewed |  | CWE-467 |
| 114 | Memory leak | Medium | CWE\_467\_UseOfSizeofOnPointerType() | Pointer 'foo' points to dynamically allocated memory. It has not been freed before the end of its scope. | Unset | Unreviewed |  | CWE-401 CWE-404 |

Table 2.36. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_468.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 117 | Use of tainted pointer | Low | CWE\_468\_IncorrectPointerScaling() | Pointer used in arithmetic operation is from an unsecure source. Pointer may be NULL or point to unknown memory. | Unset | Unreviewed |  | CWE-690 CWE-822 |

Table 2.37. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_476.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 17 | Hard-coded buffer size | Low | CWE\_476\_HostLookup() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 118 | Use of obsolete standard function | Low | CWE\_476\_HostLookup() | Obsolete routines can cause security vulnerabilities and/or portability issues. 'gethostbyaddr' is obsolete. Use 'getaddrinfo' instead. | Unset | Unreviewed |  | CWE-474 CWE-477 |

Table 2.38. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_480.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 18 | Invalid use of = operator | Medium | CWE\_480\_IsValid() |  | Unset | Unreviewed |  | CWE-480 CWE-481 |

Table 2.39. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_481.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 19 | Invalid use of = operator | Medium | CWE\_481\_IsValid() |  | Unset | Unreviewed |  | CWE-480 CWE-481 |

Table 2.40. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_482.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 20 | Invalid use of == operator | High | CWE\_482\_Push() | Use of '==' instead of '=' in a statement or missing parentheses. | Unset | Unreviewed |  | CWE-480 CWE-482 |

Table 2.41. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_484.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 26 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 21 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 22 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 23 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 24 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 25 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 27 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 28 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 29 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 30 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |
| 31 | Missing break of switch case | Low | CWE\_484\_PrintMessage() | Switch case terminates without a break statement or comment about the intentional fall through. | Unset | Unreviewed |  | CWE-484 |

Table 2.42. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_562.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 51 | Pointer or reference to stack variable leaving scope | High | CWE\_562\_GetName() | Address of local memory name escapes from its scope through its return | Unset | Unreviewed |  | CWE-562 CWE-825 |

Table 2.43. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_563.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 120 | Write without a further read | Low | CWE\_563\_UnusedVariableAssignment() | Variable 'r' is rewritten later without an intermediate read. | Unset | Unreviewed |  | CWE-398 |
| 119 | Write without a further read | Low | CWE\_563\_UnusedVariableAssignment() | Variable 'r' is never read after this point. | Unset | Unreviewed |  | CWE-398 |

Table 2.44. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_570.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 121 | Dead code | Low | CWE\_570\_HasReadWriteAccess() | If-condition always evaluates to false. Dead branch from line 10 to line 12. | Unset | Unreviewed |  | CWE-561 |

Table 2.45. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_571.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 122 | Vulnerable pseudo-random number generator | Medium | CWE\_571\_ExpressionAlwaysTrue() | 'rand' is a cryptographically weak PRNG. To make your program more secure, use 'CryptGenRandom' (Windows) or 'RAND\_bytes' (OpenSSL) instead. | Unset | Unreviewed |  | CWE-330 CWE-338 |

Table 2.46. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_587.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 32 | Function pointer assigned with absolute address | Low | CWE\_587\_ExecuteFunction() | Constant expression is used as function address. A constant address is easy to discover and vulnerable to code injection. | Unset | Unreviewed |  | CWE-587 |

Table 2.47. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_590.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 123 | Invalid free of pointer | High | CWE\_590\_FreeNonHeapMemory() | Freed pointer does not come from an adapted allocation. | Unset | Unreviewed |  | CWE-404 CWE-590 CWE-762 |

Table 2.48. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_605.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 124 | Returned value of a sensitive function not checked | High | CWE\_605\_BindSocket() | Return value of 'unlink' not checked. 'unlink' returns 0 on success or -1 on failure. To ignore this defect, cast 'unlink' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 126 | Returned value of a sensitive function not checked | High | CWE\_605\_BindSocket() | Return value of 'bind' not checked. 'bind' returns 0 on success or -1 on failure. To ignore this defect, cast 'bind' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 125 | Returned value of a sensitive function not checked | High | CWE\_605\_BindSocket() | Return value of a sensitive function saved to 'server\_sockfd', but not checked. Check the value of 'server\_sockfd' before using it. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 127 | Returned value of a sensitive function not checked | High | CWE\_605\_BindSocket() | Return value of a sensitive function saved to 'server\_sockfd', but not checked in the scope. Before return, check 'server\_sockfd' for errors or other state information. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |

Table 2.49. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_606.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 174 | Loop bounded with tainted value | Medium | CWE\_606\_Iterate() | Loop is controlled by a value from an unsecure source. Loop may be infinite. | Unset | Unreviewed |  | CWE-606 |
| 129 | Returned value of a sensitive function not checked | High | CWE\_606\_IterateFoo() | Return value of 'scanf' not checked. 'scanf' returns items to the argument list on success, possibly fewer than expected, or EOF on failure. To ignore this defect, cast 'scanf' to void. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 128 | Unsafe conversion from string to numerical value | Low | CWE\_606\_IterateFoo() | Converted value may be incorrect without additional checks. 'scanf' cannot report errors for invalid integer values associated with the conversion specifier #1. Use 'strtol', 'strtoll', 'strtoul', 'strtoull' or a related function with more robust error handling. | Unset | Unreviewed |  | CWE-20 CWE-253 CWE-676 |

Table 2.50. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_665.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 33 | Hard-coded buffer size | Low | CWE\_665\_ImproperInitialization() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 130 | Invalid use of standard library string routine | High | CWE\_665\_ImproperInitialization() | Standard function 'strcat' is called with an invalid argument.  first argument (destination) is not a valid string.  first argument (destination) may not be the correct size. | Unset | Unreviewed |  | CWE-120 CWE-227 CWE-690 |

Table 2.51. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_676.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 34 | Hard-coded buffer size | Low | CWE\_676\_ManipulateString() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 131 | Tainted NULL or non-null-terminated string | Low | CWE\_676\_ManipulateString() | Second argument to 'strcpy' is from an unsecure source. Argument may be NULL or not NULL-terminated. | Unset | Unreviewed |  | CWE-120 CWE-170 CWE-476 CWE-690 CWE-822 |

Table 2.52. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_680.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 132 | Tainted sign change conversion | Medium | CWE680\_Integer\_Overflow\_to\_Buffer\_Overflow\_\_malloc\_rand\_67b\_badSink() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |
| 133 | Tainted sign change conversion | Medium | CWE680\_Integer\_Overflow\_to\_Buffer\_Overflow\_\_malloc\_rand\_67b\_badSink() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive loop control value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |
| 134 | Non-initialized variable | High | CWE680\_Integer\_Overflow\_to\_Buffer\_Overflow\_\_malloc\_rand\_67b\_badSink() | Dereferenced value may be read before being initialized. | Unset | Unreviewed |  | CWE-456 CWE-457 CWE-908 |

Table 2.53. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_681.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 135 | Sign change integer conversion overflow | Medium | CWE\_681\_ReadData() | Conversion from int32 to unsigned int32 overflows. Valid range: [0 .. 2^32-1] | Unset | Unreviewed |  | CWE-192 CWE-194 CWE-195 CWE-196 |

Table 2.54. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_682.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 136 | Memory allocation with tainted size | Medium | CWE\_682\_AllocateImageTable() | Memory may be allocated with tainted size. Call to function malloc | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-789 |
| 137 | Tainted sign change conversion | Medium | CWE\_682\_AllocateImageTable() | Signed value is from an unsecure source and converted to an unsigned value. Overflow may yield a large positive size value. | Unset | Unreviewed |  | CWE-128 CWE-131 CWE-192 CWE-194 CWE-195 |

Table 2.55. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_685.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 35 | Format string specifiers and arguments mismatch | Low | CWE685\_FunctionCallWithIncorrectNumberOfArguments() | The format string requires additional arguments | Unset | Unreviewed |  | CWE-683 CWE-685 CWE-686 |

Table 2.56. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_686.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 36 | Hard-coded buffer size | Low | CWE\_686\_WrongArgumentsFuncPointer() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 138 | Write without a further read | Low | CWE\_686\_WrongArgumentsFuncPointer() | Variable 'a' is never read after this point. | Unset | Unreviewed |  | CWE-398 |

Table 2.57. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_688.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 37 | Format string specifiers and arguments mismatch | Low | CWE688\_FunctionCallWithIncorrectVariable() | Mismatch between the argument of type 'int' and the corresponding format specifier '%s'. | Unset | Unreviewed |  | CWE-683 CWE-685 CWE-686 |

Table 2.58. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_690.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 38 | Hard-coded buffer size | Low | CWE690\_HostLookup() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 139 | Use of obsolete standard function | Low | CWE690\_HostLookup() | Obsolete routines can cause security vulnerabilities and/or portability issues. 'gethostbyaddr' is obsolete. Use 'getaddrinfo' instead. | Unset | Unreviewed |  | CWE-474 CWE-477 |

Table 2.59. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_704.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 140 | Integer conversion overflow | High | CWE704\_IncorrectTypeConversion() | Conversion from int64 to int32 overflows. Valid range: [-2^31 .. 2^31-1] | Unset | Unreviewed |  | CWE-128 CWE-189 CWE-190 CWE-191 CWE-192 CWE-197 |
| 144 | Write without a further read | Low | CWE704\_IncorrectTypeConversion() | Variable 'ii' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 143 | Write without a further read | Low | CWE704\_IncorrectTypeConversion() | Variable 'j' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 142 | Write without a further read | Low | CWE704\_IncorrectTypeConversion() | Variable 'c' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 141 | Write without a further read | Low | CWE704\_IncorrectTypeConversion() | Variable 'int\_ptr' is never read after this point. | Unset | Unreviewed |  | CWE-398 |

Table 2.60. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_761.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 145 | Invalid use of standard library string routine | High | CWE761\_ContainsChar() | Standard function 'strcpy' may be called with an invalid argument.  first argument (destination) may not be the correct size. | Unset | Unreviewed |  | CWE-120 CWE-227 CWE-690 |
| 146 | Unprotected dynamic memory allocation | Low | CWE761\_ContainsChar() | Possible failure of dynamic allocation (out of memory) may not have been checked. | Unset | Unreviewed |  | CWE-253 CWE-690 CWE-789 |

Table 2.61. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_787.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 39 | Hard-coded buffer size | Low | CWE787\_OutOfBoundsWrite() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 151 | Write without a further read | Low | CWE787\_OutOfBoundsWrite() | Variable 'id\_sequence' is rewritten later without an intermediate read. | Unset | Unreviewed |  | CWE-398 |
| 150 | Write without a further read | Low | CWE787\_OutOfBoundsWrite() | Variable 'id\_sequence' is rewritten later without an intermediate read. | Unset | Unreviewed |  | CWE-398 |
| 149 | Write without a further read | Low | CWE787\_OutOfBoundsWrite() | Variable 'id\_sequence' is rewritten later without an intermediate read. | Unset | Unreviewed |  | CWE-398 |
| 148 | Write without a further read | Low | CWE787\_OutOfBoundsWrite() | Variable 'id\_sequence' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 147 | Array access out of bounds | High | CWE787\_OutOfBoundsWrite() | Attempt to access to array element 3.  Valid index range: [0 .. 2]. | Unset | Unreviewed |  | CWE-119 CWE-131 CWE-466 |

Table 2.62. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_788.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 40 | Hard-coded buffer size | Low | CWE788\_HostLookup() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 152 | Use of obsolete standard function | Low | CWE788\_HostLookup() | Obsolete routines can cause security vulnerabilities and/or portability issues. 'gethostbyaddr' is obsolete. Use 'getaddrinfo' instead. | Unset | Unreviewed |  | CWE-474 CWE-477 |

Table 2.63. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_789.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 44 | Declaration mismatch | High | File Scope | Global declaration of 'GetUntrustedInt' function has a type incompatible with its definition. This defect occurs when linking the 2 translation units: D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_789.c D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_192.c | Unset | Unreviewed |  | CWE-685 CWE-686 |
| 52 | Memory leak | Medium | CWE789\_UncontrolledMemoryAllocation() | Pointer 'string' points to dynamically allocated memory. It has not been freed before the end of its scope. | Unset | Unreviewed |  | CWE-401 CWE-404 |

Table 2.64. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_805.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 43 | Hard-coded buffer size | Low | CWE805\_HostLookup() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 153 | Use of obsolete standard function | Low | CWE805\_HostLookup() | Obsolete routines can cause security vulnerabilities and/or portability issues. 'gethostbyaddr' is obsolete. Use 'getaddrinfo' instead. | Unset | Unreviewed |  | CWE-474 CWE-477 |

Table 2.65. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_806.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 42 | Hard-coded buffer size | Low | CWE806\_BufferAccessUsingSourceSize() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 41 | Hard-coded buffer size | Low | CWE806\_BufferAccessUsingSourceSize() | Buffer size is hard coded instead of a symbolic constant. Hard-coded buffer size increases maintenance costs and security risks. | Unset | Unreviewed |  | CWE-547 |
| 154 | Invalid use of standard library string routine | High | CWE806\_BufferAccessUsingSourceSize() | Standard function 'strncpy' is called with an invalid argument.  first argument (destination) is not allocated enough to receive the copied string. | Unset | Unreviewed |  | CWE-120 CWE-227 CWE-690 |

Table 2.66. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_824.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 156 | Write without a further read | Low | CWE824\_UninitializedPointer() | Variable 'ret' is never read after this point. | Unset | Unreviewed |  | CWE-398 |
| 155 | Non-initialized pointer | High | CWE824\_UninitializedPointer() | Local pointer 'p' is read before being initialized. | Unset | Unreviewed |  | CWE-456 CWE-457 CWE-824 CWE-908 |

Table 2.67. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_835.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 157 | Returned value of a sensitive function not checked | High | CWE835\_ProcessMessagesFromServer() | Return value of a sensitive function saved to 'servsock', but not checked. Check the value of 'servsock' before using it. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |
| 158 | Returned value of a sensitive function not checked | High | CWE835\_ProcessMessagesFromServer() | Return value of a sensitive function saved to 'servsock', but not checked in the scope. Before return, check 'servsock' for errors or other state information. | Unset | Unreviewed |  | CWE-252 CWE-253 CWE-690 CWE-754 |

Table 2.68. D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_843.c

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Defect** | **Impact** | **Function** | **Detail** | **Severity** | **Status** | **Comment** | **CWE ID** |
| 159 | Dead code | Low | CWE843\_TypeConfusion() | If-condition always evaluates to true. Dead branch from line 19 to line 21. | Unset | Unreviewed |  | CWE-561 |

Chapter 3. Appendix 1 - Configuration Settings

Polyspace Settings

|  |  |
| --- | --- |
| **Option** | **Value** |
| -author | YangLiMin |
| -bug-finder | true |
| -checkers | BAD\_EQUAL\_EQUAL\_USE, BAD\_EQUAL\_USE, BAD\_FILE\_ACCESS\_MODE\_STATUS, BAD\_FLOAT\_OP, BAD\_FREE, BAD\_INT\_PTR\_CAST, BAD\_LOCK, BAD\_NETWORK\_CONNECT\_ORDER, BAD\_PLAIN\_CHAR\_USE, BAD\_PRIVILEGE\_DROP\_ORDER, BAD\_PTR\_SCALING, BAD\_UMASK, BAD\_UNLOCK, BITWISE\_ARITH\_MIX, BITWISE\_NEG, BLOCKING\_WHILE\_LOCKED, CHARACTER\_MISUSE, CHAR\_EOF\_CONFUSED, CHROOT\_MISUSE, CLOSED\_RESOURCE\_USE, CONSTANT\_OBJECT\_WRITE, CRYPTO\_CIPHER\_BAD\_FUNCTION, CRYPTO\_CIPHER\_CONSTANT\_IV, CRYPTO\_CIPHER\_CONSTANT\_KEY, CRYPTO\_CIPHER\_NO\_ALGORITHM, CRYPTO\_CIPHER\_NO\_DATA, CRYPTO\_CIPHER\_NO\_FINAL, CRYPTO\_CIPHER\_NO\_IV, CRYPTO\_CIPHER\_NO\_KEY, CRYPTO\_CIPHER\_PREDICTABLE\_IV, CRYPTO\_CIPHER\_PREDICTABLE\_KEY, CRYPTO\_CIPHER\_WEAK\_CIPHER, CRYPTO\_CIPHER\_WEAK\_MODE, CRYPTO\_MD\_BAD\_FUNCTION, CRYPTO\_MD\_NO\_ALGORITHM, CRYPTO\_MD\_NO\_DATA, CRYPTO\_MD\_NO\_FINAL, CRYPTO\_MD\_NO\_SALT, CRYPTO\_MD\_WEAK\_HASH, CRYPTO\_PKEY\_INCORRECT\_INIT, CRYPTO\_PKEY\_INCORRECT\_KEY, CRYPTO\_PKEY\_NO\_DATA, CRYPTO\_PKEY\_NO\_PARAMS, CRYPTO\_PKEY\_NO\_PEER, CRYPTO\_PKEY\_NO\_PRIVATE\_KEY, CRYPTO\_PKEY\_NO\_PUBLIC\_KEY, CRYPTO\_PKEY\_WEAK\_PARAMS, CRYPTO\_RSA\_BAD\_PADDING, CRYPTO\_RSA\_LOW\_EXPONENT, CRYPTO\_RSA\_NO\_BLINDING, CRYPTO\_RSA\_NO\_PADDING, CRYPTO\_RSA\_WEAK\_PADDING, CRYPTO\_SSL\_BAD\_ROLE, CRYPTO\_SSL\_CERT\_NOT\_CHECKED, CRYPTO\_SSL\_HOSTNAME\_NOT\_CHECKED, CRYPTO\_SSL\_NO\_CA, CRYPTO\_SSL\_NO\_CERTIFICATE, CRYPTO\_SSL\_NO\_PRIVATE\_KEY, CRYPTO\_SSL\_NO\_ROLE, CRYPTO\_SSL\_WEAK\_PROTOCOL, DANGEROUS\_PERMISSIONS, DANGEROUS\_STD\_FUNC, DATA\_LENGTH\_MISMATCH, DATA\_RACE, DATA\_RACE\_ALL, DATA\_RACE\_STD\_LIB, DEADLOCK, DEAD\_CODE, DECL\_MISMATCH, DESTROY\_LOCKED, DOUBLE\_DEALLOCATION, DOUBLE\_LOCK, DOUBLE\_RESOURCE\_CLOSE, DOUBLE\_RESOURCE\_OPEN, DOUBLE\_UNLOCK, ERRNO\_MISUSE, ERRNO\_NOT\_CHECKED, EXIT\_ABNORMAL\_HANDLER, FILE\_EXPOSURE\_TO\_CHILD, FLOAT\_ABSORPTION, FLOAT\_CONV\_OVFL, FLOAT\_OVFL, FLOAT\_STD\_LIB, FLOAT\_ZERO\_DIV, FREED\_PTR, FUNC\_PTR\_ABSOLUTE\_ADDR, HARD\_CODED\_BUFFER\_SIZE, HARD\_CODED\_LOOP\_BOUNDARY, HARD\_CODED\_MEM\_SIZE, IMPROPER\_ARRAY\_INIT, INAPPROPRIATE\_IO\_ON\_DEVICE, INCORRECT\_INDENTATION, INT\_CONSTANT\_OVFL, INT\_CONV\_OVFL, INT\_OVFL, INT\_PRECISION\_EXCEEDED, INT\_STD\_LIB, INT\_TO\_FLOAT\_PRECISION\_LOSS, INT\_ZERO\_DIV, INVALID\_ENV\_POINTER, INVALID\_MEMORY\_ASSUMPTION, INVALID\_OPERATION\_ON\_BOOLEAN, INVALID\_VA\_LIST\_ARG, LOCAL\_ADDR\_ESCAPE, MEMCMP\_PADDING\_DATA, MEMCMP\_STRINGS, MEMSET\_INVALID\_SIZE, MEMSET\_INVALID\_VALUE, MEM\_LEAK, MEM\_STD\_LIB, MISSING\_BYTESWAP, MISSING\_ERRNO\_RESET, MISSING\_FREED\_PTR\_RESET, MISSING\_NULL\_CHAR, MISSING\_PRIVILEGE\_DROP\_CHECK, MISSING\_SWITCH\_BREAK, MISSING\_SWITCH\_CASE, NARROW\_WIDE\_STR\_MISUSE, NON\_INIT\_PTR, NON\_INIT\_VAR, NON\_POSITIVE\_VLA\_SIZE, NON\_SECURE\_TEMP\_FILE, NULL\_PTR, OBJECT\_SIZE\_MISMATCH, OBSOLETE\_STD\_FUNC, OPERATOR\_PRECEDENCE, OTHER\_STD\_LIB, OUT\_BOUND\_ARRAY, OUT\_BOUND\_PTR, OVERLAPPING\_ASSIGN, OVERLAPPING\_COPY, PATH\_BUFFER\_OVERFLOW, PATH\_TRAVERSAL, PTR\_CAST, PTR\_SIZEOF\_MISMATCH, PTR\_TO\_DIFF\_ARRAY, PUTENV\_AUTO\_VAR, QUALIFIER\_MISMATCH, RAND\_SEED\_CONSTANT, RAND\_SEED\_PREDICTABLE, READLINK\_MISUSE, RELATIVE\_PATH\_CMD, RELATIVE\_PATH\_LIB, RESOURCE\_LEAK, RETURN\_NOT\_CHECKED, SEMICOLON\_CTRL\_STMT\_SAME\_LINE, SENSITIVE\_DATA\_PRINT, SENSITIVE\_HEAP\_NOT\_CLEARED, SENSITIVE\_STACK\_NOT\_CLEARED, SETJMP\_LONGJMP\_USE, SHIFT\_NEG, SHIFT\_OVFL, SIGN\_CHANGE, SIG\_HANDLER\_ASYNC\_UNSAFE, SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT, SIG\_HANDLER\_CALLING\_SIGNAL, SIG\_HANDLER\_COMP\_EXCP\_RETURN, SIG\_HANDLER\_SHARED\_OBJECT, SIZEOF\_MISUSE, STD\_FUNC\_ARG\_MISMATCH, STRING\_FORMAT, STRLIB\_BUFFER\_OVERFLOW, STRLIB\_BUFFER\_UNDERFLOW, STR\_FORMAT\_BUFFER\_OVERFLOW, STR\_STD\_LIB, TAINTED\_ARRAY\_INDEX, TAINTED\_ENV\_VARIABLE, TAINTED\_EXTERNAL\_CMD, TAINTED\_HOSTID, TAINTED\_INT\_DIVISION, TAINTED\_INT\_MOD, TAINTED\_LOOP\_BOUNDARY, TAINTED\_MEMORY\_ALLOC\_SIZE, TAINTED\_PATH\_CMD, TAINTED\_PATH\_LIB, TAINTED\_PTR, TAINTED\_PTR\_OFFSET, TAINTED\_SIGN\_CHANGE, TAINTED\_STRING, TAINTED\_STRING\_FORMAT, TAINTED\_VLA\_SIZE, TEMP\_OBJECT\_ACCESS, THREAD\_MEM\_LEAK, TOCTOU, TOO\_MANY\_VA\_ARG\_CALLS, UINT\_CONSTANT\_OVFL, UINT\_CONV\_OVFL, UINT\_OVFL, UNCALLED\_FUNC, UNPROTECTED\_MEMORY\_ALLOCATION, UNREACHABLE, UNSAFE\_STD\_CRYPT, UNSAFE\_STD\_FUNC, UNSAFE\_STR\_TO\_NUMERIC, UNSAFE\_SYSTEM\_CALL, USELESS\_WRITE, VA\_ARG\_INCORRECT\_TYPE, VULNERABLE\_PRNG, WIN\_MISMATCH\_DEALLOC, WRITE\_INTERNAL\_BUFFER\_RETURNED\_FROM\_STD\_FUNC |
| -compiler | generic |
| -date | 02/12/2024 |
| -dos | true |
| -I | D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code |
| -import-comments | C:\Users\yanglimin\Documents\Polyspace\_Workspace\Module\_1\BF\_Result\_4 |
| -lang | C |
| -prog | cwe |
| -report-output-format | Word |
| -report-template | Polyspace-Doc\SecurityCWE.rpt |
| -results-dir | C:\Users\yanglimin\Documents\Polyspace\_Workspace\Module\_1\BF\_Result\_5 |
| -target | i386 |
| -verif-version | 1.0 |

Security Standard to Polyspace Result Map

Table 3.1. Security Standard to Polyspace Result Map

|  |  |
| --- | --- |
| **CWE** | **Polyspace Result** |
| [CWE-15] One or more system settings or configuration elements can be externally controlled by a user. | [TAINTED\_ENV\_VARIABLE] Use of externally controlled environment variable [TAINTED\_HOSTID] Host change using externally controlled elements |
| [CWE-20] The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program. | [UNSAFE\_STR\_TO\_NUMERIC] Unsafe conversion from string to numerical value |
| [CWE-22] The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. | [PATH\_TRAVERSAL] Vulnerable path manipulation |
| [CWE-23] The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory. | [PATH\_TRAVERSAL] Vulnerable path manipulation |
| [CWE-36] The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize absolute path sequences such as "/abs/path" that can resolve to a location that is outside of that directory. | [PATH\_TRAVERSAL] Vulnerable path manipulation |
| [CWE-67] The software constructs pathnames from user input, but it does not handle or incorrectly handles a pathname containing a Windows device name such as AUX or CON. This typically leads to denial of service or an information exposure when the application attempts to process the pathname as a regular file. | [INAPPROPRIATE\_IO\_ON\_DEVICE] Inappropriate I/O operation on device files |
| [CWE-77] The software constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. | [TAINTED\_EXTERNAL\_CMD] Execution of externally controlled command |
| [CWE-78] The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. | [TAINTED\_EXTERNAL\_CMD] Execution of externally controlled command [UNSAFE\_SYSTEM\_CALL] Unsafe call to a system function |
| [CWE-88] The software does not sufficiently delimit the arguments being passed to a component in another control sphere, allowing alternate arguments to be provided, leading to potentially security-relevant changes. | [TAINTED\_EXTERNAL\_CMD] Execution of externally controlled command [UNSAFE\_SYSTEM\_CALL] Unsafe call to a system function |
| [CWE-114] Executing commands or loading libraries from an untrusted source or in an untrusted environment can cause an application to execute malicious commands (and payloads) on behalf of an attacker. | [RELATIVE\_PATH\_CMD] Execution of a binary from a relative path can be controlled by an external actor [RELATIVE\_PATH\_LIB] Load of library from a relative path can be controlled by an external actor [TAINTED\_EXTERNAL\_CMD] Execution of externally controlled command [TAINTED\_PATH\_CMD] Command executed from externally controlled path [TAINTED\_PATH\_LIB] Library loaded from externally controlled path |
| [CWE-119] The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer. | [OUT\_BOUND\_ARRAY] Array access out of bounds [OUT\_BOUND\_PTR] Pointer access out of bounds |
| [CWE-120] The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. | [MEM\_STD\_LIB] Invalid use of standard library memory routine [STR\_STD\_LIB] Invalid use of standard library string routine [TAINTED\_STRING] Tainted NULL or non-null-terminated string |
| [CWE-121] A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). | [STRLIB\_BUFFER\_OVERFLOW] Destination buffer overflow in string manipulation [TAINTED\_ARRAY\_INDEX] Array access with tainted index |
| [CWE-122] A heap overflow condition is a buffer overflow, where the buffer that can be overwritten is allocated in the heap portion of memory, generally meaning that the buffer was allocated using a routine such as malloc(). | [TAINTED\_PTR\_OFFSET] Pointer dereference with tainted offset |
| [CWE-124] The software writes to a buffer using an index or pointer that references a memory location prior to the beginning of the buffer. | [STR\_FORMAT\_BUFFER\_OVERFLOW] Buffer overflow from incorrect string format specifier [STRLIB\_BUFFER\_UNDERFLOW] Destination buffer underflow in string manipulation [TAINTED\_ARRAY\_INDEX] Array access with tainted index [TAINTED\_PTR\_OFFSET] Pointer dereference with tainted offset |
| [CWE-125] The software reads data past the end, or before the beginning, of the intended buffer. | [STR\_FORMAT\_BUFFER\_OVERFLOW] Buffer overflow from incorrect string format specifier [STRLIB\_BUFFER\_OVERFLOW] Destination buffer overflow in string manipulation [TAINTED\_ARRAY\_INDEX] Array access with tainted index |
| [CWE-126] The software reads from a buffer using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer. | [STR\_FORMAT\_BUFFER\_OVERFLOW] Buffer overflow from incorrect string format specifier |
| [CWE-127] The software reads from a buffer using buffer access mechanisms such as indexes or pointers that reference memory locations prior to the targeted buffer. | [STR\_FORMAT\_BUFFER\_OVERFLOW] Buffer overflow from incorrect string format specifier |
| [CWE-128] Wrap around errors occur whenever a value is incremented past the maximum value for its type and therefore "wraps around" to a very small, negative, or undefined value. | [INT\_OVFL] Integer overflow [INT\_CONSTANT\_OVFL] Integer constant overflow [UINT\_OVFL] Unsigned integer overflow [UINT\_CONSTANT\_OVFL] Unsigned integer constant overflow [INT\_CONV\_OVFL] Integer conversion overflow [UINT\_CONV\_OVFL] Unsigned integer conversion overflow [TAINTED\_SIGN\_CHANGE] Tainted sign change conversion [TAINTED\_MEMORY\_ALLOC\_SIZE] Memory allocation with tainted size [TAINTED\_VLA\_SIZE] Tainted size of variable length array |
| [CWE-129] The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array. | [TAINTED\_ARRAY\_INDEX] Array access with tainted index [TAINTED\_PTR\_OFFSET] Pointer dereference with tainted offset |
| [CWE-130] The software parses a formatted message or structure, but it does not handle or incorrectly handles a length field that is inconsistent with the actual length of the associated data. | [DATA\_LENGTH\_MISMATCH] Mismatch between data length and size |
| [CWE-131] The software does not correctly calculate the size to be used when allocating a buffer, which could lead to a buffer overflow. | [UINT\_OVFL] Unsigned integer overflow [UINT\_CONV\_OVFL] Unsigned integer conversion overflow [TAINTED\_SIGN\_CHANGE] Tainted sign change conversion [TAINTED\_MEMORY\_ALLOC\_SIZE] Memory allocation with tainted size [TAINTED\_VLA\_SIZE] Tainted size of variable length array [OUT\_BOUND\_PTR] Pointer access out of bounds [OUT\_BOUND\_ARRAY] Array access out of bounds |
| [CWE-134] The software uses externally-controlled format strings in printf-style functions, which can lead to buffer overflows or data representation problems. | [TAINTED\_STRING\_FORMAT] Tainted string format |
| [CWE-135] The software does not correctly calculate the length of strings that can contain wide or multi-byte characters. | [NARROW\_WIDE\_STR\_MISUSE] Misuse of narrow or wide character string [PTR\_CAST] Unreliable cast of pointer [STRLIB\_BUFFER\_OVERFLOW] Destination buffer overflow in string manipulation |
| [CWE-170] The software does not terminate or incorrectly terminates a string or array with a null character or equivalent terminator. | [MISSING\_NULL\_CHAR] Missing null in string array [READLINK\_MISUSE] Misuse of readlink() [TAINTED\_STRING] Tainted NULL or non-null-terminated string |
| [CWE-188] The software makes invalid assumptions about how protocol data or memory is organized at a lower level, resulting in unintended program behavior. | [INVALID\_MEMORY\_ASSUMPTION] Invalid assumptions about memory organization [MEMCMP\_PADDING\_DATA] Memory comparison of padding data [MEMCMP\_STRINGS] Memory comparison of strings [OUT\_BOUND\_PTR] Pointer access out of bounds [MISSING\_BYTESWAP] Missing byte reordering when transferring data |
| [CWE-189] Weaknesses in this category are related to improper calculation or conversion of numbers. | [INT\_CONV\_OVFL] Integer conversion overflow [INT\_OVFL] Integer overflow [INT\_CONSTANT\_OVFL] Integer constant overflow [SHIFT\_OVFL] Shift operation overflow [SHIFT\_NEG] Shift of a negative value [UINT\_CONV\_OVFL] Unsigned integer conversion overflow [UINT\_OVFL] Unsigned integer overflow [UINT\_CONSTANT\_OVFL] Unsigned integer constant overflow [FLOAT\_OVFL] Float overflow [FLOAT\_CONV\_OVFL] Float conversion overflow [FLOAT\_ABSORPTION] Absorption of float operand [INT\_ZERO\_DIV] Integer division by zero [FLOAT\_ZERO\_DIV] Float division by zero [TAINTED\_INT\_DIVISION] Tainted division operand [INT\_TO\_FLOAT\_PRECISION\_LOSS] Precision loss in integer to float conversion |
| [CWE-190] The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control. | [INT\_CONV\_OVFL] Integer conversion overflow [INT\_OVFL] Integer overflow [INT\_CONSTANT\_OVFL] Integer constant overflow [SHIFT\_OVFL] Shift operation overflow [TAINTED\_INT\_DIVISION] Tainted division operand [UINT\_CONV\_OVFL] Unsigned integer conversion overflow [UINT\_OVFL] Unsigned integer overflow [UINT\_CONSTANT\_OVFL] Unsigned integer constant overflow [INT\_PRECISION\_EXCEEDED] Integer precision exceeded [INVALID\_OPERATION\_ON\_BOOLEAN] Possible invalid operation on boolean operand |
| [CWE-191] The product subtracts one value from another, such that the result is less than the minimum allowable integer value, which produces a value that is not equal to the correct result. | [INT\_CONV\_OVFL] Integer conversion overflow [INT\_OVFL] Integer overflow [INT\_CONSTANT\_OVFL] Integer constant overflow [UINT\_CONV\_OVFL] Unsigned integer conversion overflow [UINT\_OVFL] Unsigned integer overflow [UINT\_CONSTANT\_OVFL] Unsigned integer constant overflow |
| [CWE-192] Integer coercion refers to a set of flaws pertaining to the type casting, extension, or truncation of primitive data types. | [INT\_CONV\_OVFL] Integer conversion overflow [INT\_OVFL] Integer overflow [UINT\_CONV\_OVFL] Unsigned integer conversion overflow [UINT\_OVFL] Unsigned integer overflow [SIGN\_CHANGE] Sign change integer conversion overflow [TAINTED\_SIGN\_CHANGE] Tainted sign change conversion |
| [CWE-194] The software performs an operation on a number that causes it to be sign extended when it is transformed into a larger data type. When the original number is negative, this can produce unexpected values that lead to resultant weaknesses. | [SIGN\_CHANGE] Sign change integer conversion overflow [TAINTED\_SIGN\_CHANGE] Tainted sign change conversion |
| [CWE-195] The software uses a signed primitive and performs a cast to an unsigned primitive, which can produce an unexpected value if the value of the signed primitive can not be represented using an unsigned primitive. | [SIGN\_CHANGE] Sign change integer conversion overflow [TAINTED\_SIGN\_CHANGE] Tainted sign change conversion |
| [CWE-196] The software uses an unsigned primitive and performs a cast to a signed primitive, which can produce an unexpected value if the value of the unsigned primitive can not be represented using a signed primitive. | [SIGN\_CHANGE] Sign change integer conversion overflow |
| [CWE-197] Truncation errors occur when a primitive is cast to a primitive of a smaller size and data is lost in the conversion. | [FLOAT\_CONV\_OVFL] Float conversion overflow [INT\_CONV\_OVFL] Integer conversion overflow [UINT\_CONV\_OVFL] Unsigned integer conversion overflow |
| [CWE-198] The software receives input from an upstream component, but it does not account for byte ordering (e.g. big-endian and little-endian) when processing the input, causing an incorrect number or value to be used. | [MISSING\_BYTESWAP] Missing byte reordering when transferring data |
| [CWE-226] The software does not fully clear previously used information in a data structure, file, or other resource, before making that resource available to a party in another control sphere. | [SENSITIVE\_STACK\_NOT\_CLEARED] Uncleared sensitive data in stack |
| [CWE-227] The software uses an API in a manner contrary to its intended use. | [CONSTANT\_OBJECT\_WRITE] Writing to const qualified object [FLOAT\_STD\_LIB] Invalid use of standard library floating point routine [INT\_STD\_LIB] Invalid use of standard library integer routine [MEM\_STD\_LIB] Invalid use of standard library memory routine [OTHER\_STD\_LIB] Invalid use of standard library routine [STR\_STD\_LIB] Invalid use of standard library string routine |
| [CWE-240] The software does not handle or incorrectly handles when two or more structural elements should be consistent, but are not. | [DATA\_LENGTH\_MISMATCH] Mismatch between data length and size |
| [CWE-242] The program calls a function that can never be guaranteed to work safely. | [DANGEROUS\_STD\_FUNC] Use of dangerous standard function |
| [CWE-243] The program uses the chroot() system call to create a jail, but does not change the working directory afterward. This does not prevent access to files outside of the jail. | [CHROOT\_MISUSE] File manipulation after chroot() without chdir("/") |
| [CWE-244] Using realloc() to resize buffers that store sensitive information can leave the sensitive information exposed to attack, because it is not removed from memory. | [SENSITIVE\_HEAP\_NOT\_CLEARED] Sensitive heap memory not cleared before release |
| [CWE-250] The software performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. | [BAD\_PRIVILEGE\_DROP\_ORDER] Bad order of dropping privileges [MISSING\_PRIVILEGE\_DROP\_CHECK] Privilege drop not verified |
| [CWE-251] Functions that manipulate strings encourage buffer overflows. | [STRLIB\_BUFFER\_OVERFLOW] Destination buffer overflow in string manipulation |
| [CWE-252] The software does not check the return value from a method or function, which can prevent it from detecting unexpected states and conditions. | [RETURN\_NOT\_CHECKED] Returned value of a sensitive function not checked |
| [CWE-253] The software incorrectly checks a return value from a function, which prevents the software from detecting errors or exceptional conditions. | [RETURN\_NOT\_CHECKED] Returned value of a sensitive function not checked [ERRNO\_NOT\_CHECKED] Errno not checked [MISSING\_ERRNO\_RESET] Errno not reset [UNPROTECTED\_MEMORY\_ALLOCATION] Unprotected dynamic memory allocation [UNSAFE\_STR\_TO\_NUMERIC] Unsafe conversion from string to numerical value |
| [CWE-273] The software attempts to drop privileges but does not check or incorrectly checks to see if the drop succeeded. | [MISSING\_PRIVILEGE\_DROP\_CHECK] Privilege drop not verified |
| [CWE-287] When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. | [CRYPTO\_SSL\_CERT\_NOT\_CHECKED] X.509 peer certificate not checked |
| [CWE-297] The software communicates with a host that provides a certificate, but the software does not properly ensure that the certificate is actually associated with that host. | [CRYPTO\_SSL\_HOSTNAME\_NOT\_CHECKED] Server certificate common name not checked |
| [CWE-304] The software implements an authentication technique, but it skips a step that weakens the technique. | [CRYPTO\_SSL\_NO\_ROLE] TLS/SSL connection method not set |
| [CWE-310] Weaknesses in this category are related to the use of cryptography. | [CRYPTO\_CIPHER\_CONSTANT\_IV] Constant block cipher initialization vector [CRYPTO\_CIPHER\_CONSTANT\_KEY] Constant cipher key [CRYPTO\_CIPHER\_NO\_ALGORITHM] Missing cipher algorithm [CRYPTO\_CIPHER\_NO\_IV] Missing block cipher initialization vector [CRYPTO\_CIPHER\_NO\_KEY] Missing cipher key [CRYPTO\_CIPHER\_PREDICTABLE\_IV] Predictable block cipher initialization vector [CRYPTO\_CIPHER\_PREDICTABLE\_KEY] Predictable cipher key [CRYPTO\_CIPHER\_WEAK\_CIPHER] Weak cipher algorithm [CRYPTO\_CIPHER\_WEAK\_MODE] Weak cipher mode [CRYPTO\_PKEY\_NO\_PUBLIC\_KEY] Missing public key [CRYPTO\_PKEY\_NO\_PEER] Missing peer key [CRYPTO\_PKEY\_NO\_PRIVATE\_KEY] Missing private key [CRYPTO\_PKEY\_NO\_PARAMS] Missing parameters for key generation [CRYPTO\_PKEY\_WEAK\_PARAMS] Nonsecure parameters for key generation [CRYPTO\_RSA\_LOW\_EXPONENT] Nonsecure RSA public exponent [CRYPTO\_PKEY\_NO\_DATA] Missing data for encryption, decryption or signing operation [CRYPTO\_PKEY\_INCORRECT\_KEY] Incorrect key for cryptographic algorithm [CRYPTO\_PKEY\_INCORRECT\_INIT] Context initialized incorrectly for cryptographic operation [CRYPTO\_RSA\_NO\_BLINDING] Missing blinding for RSA algorithm [CRYPTO\_RSA\_NO\_PADDING] Missing padding for RSA algorithm [CRYPTO\_RSA\_WEAK\_PADDING] Weak padding for RSA algorithm [CRYPTO\_RSA\_BAD\_PADDING] Incompatible padding for RSA algorithm operation [CRYPTO\_MD\_WEAK\_HASH] Nonsecure hash algorithm [CRYPTO\_MD\_BAD\_FUNCTION] Context initialized incorrectly for digest operation [CRYPTO\_SSL\_WEAK\_PROTOCOL] Nonsecure SSL/TLS protocol [CRYPTO\_SSL\_NO\_CA] Missing certification authority list [CRYPTO\_SSL\_NO\_CERTIFICATE] Missing X.509 certificate |
| [CWE-311] The software does not encrypt sensitive or critical information before storage or transmission. | [CRYPTO\_CIPHER\_NO\_DATA] Missing cipher data to process [CRYPTO\_CIPHER\_NO\_FINAL] Missing cipher final step |
| [CWE-312] The application stores sensitive information in cleartext within a resource that might be accessible to another control sphere. | [SENSITIVE\_STACK\_NOT\_CLEARED] Uncleared sensitive data in stack [SENSITIVE\_HEAP\_NOT\_CLEARED] Sensitive heap memory not cleared before release |
| [CWE-316] The application stores sensitive information in cleartext in memory. | [SENSITIVE\_STACK\_NOT\_CLEARED] Uncleared sensitive data in stack [SENSITIVE\_HEAP\_NOT\_CLEARED] Sensitive heap memory not cleared before release |
| [CWE-320] Weaknesses in this category are related to errors in the management of cryptographic keys. | [CRYPTO\_CIPHER\_CONSTANT\_KEY] Constant cipher key [CRYPTO\_CIPHER\_NO\_KEY] Missing cipher key [CRYPTO\_PKEY\_NO\_PUBLIC\_KEY] Missing public key [CRYPTO\_PKEY\_NO\_PEER] Missing peer key [CRYPTO\_PKEY\_NO\_PRIVATE\_KEY] Missing private key |
| [CWE-321] The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered. | [CRYPTO\_CIPHER\_CONSTANT\_KEY] Constant cipher key |
| [CWE-322] The software performs a key exchange with an actor without verifying the identity of that actor. | [CRYPTO\_SSL\_NO\_ROLE] TLS/SSL connection method not set |
| [CWE-325] The software does not implement a required step in a cryptographic algorithm, resulting in weaker encryption than advertised by that algorithm. | [CRYPTO\_CIPHER\_NO\_DATA] Missing cipher data to process [CRYPTO\_CIPHER\_NO\_FINAL] Missing cipher final step [CRYPTO\_PKEY\_NO\_DATA] Missing data for encryption, decryption or signing operation [CRYPTO\_PKEY\_NO\_PARAMS] Missing parameters for key generation [CRYPTO\_PKEY\_INCORRECT\_KEY] Incorrect key for cryptographic algorithm [CRYPTO\_PKEY\_INCORRECT\_INIT] Context initialized incorrectly for cryptographic operation [CRYPTO\_MD\_NO\_DATA] No data added into context |
| [CWE-326] The software stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required. | [CRYPTO\_CIPHER\_CONSTANT\_IV] Constant block cipher initialization vector [CRYPTO\_CIPHER\_CONSTANT\_KEY] Constant cipher key [CRYPTO\_CIPHER\_NO\_IV] Missing block cipher initialization vector [CRYPTO\_CIPHER\_PREDICTABLE\_KEY] Predictable cipher key [CRYPTO\_CIPHER\_WEAK\_CIPHER] Weak cipher algorithm [CRYPTO\_CIPHER\_WEAK\_MODE] Weak cipher mode [CRYPTO\_PKEY\_WEAK\_PARAMS] Nonsecure parameters for key generation [CRYPTO\_RSA\_NO\_BLINDING] Missing blinding for RSA algorithm [CRYPTO\_RSA\_NO\_PADDING] Missing padding for RSA algorithm [CRYPTO\_RSA\_WEAK\_PADDING] Weak padding for RSA algorithm [CRYPTO\_RSA\_LOW\_EXPONENT] Nonsecure RSA public exponent |
| [CWE-327] The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive information. | [UNSAFE\_STD\_CRYPT] Unsafe standard encryption function [CRYPTO\_CIPHER\_WEAK\_CIPHER] Weak cipher algorithm [CRYPTO\_CIPHER\_WEAK\_MODE] Weak cipher mode [CRYPTO\_PKEY\_WEAK\_PARAMS] Nonsecure parameters for key generation [CRYPTO\_RSA\_NO\_PADDING] Missing padding for RSA algorithm [CRYPTO\_RSA\_WEAK\_PADDING] Weak padding for RSA algorithm [CRYPTO\_RSA\_LOW\_EXPONENT] Nonsecure RSA public exponent [CRYPTO\_MD\_WEAK\_HASH] Nonsecure hash algorithm [CRYPTO\_SSL\_WEAK\_PROTOCOL] Nonsecure SSL/TLS protocol |
| [CWE-328] The product uses a hashing algorithm that produces a hash value that can be used to determine the original input, or to find an input that can produce the same hash, more efficiently than brute force techniques. | [CRYPTO\_MD\_WEAK\_HASH] Nonsecure hash algorithm |
| [CWE-329] Not using a random initialization Vector (IV) with Cipher Block Chaining (CBC) Mode causes algorithms to be susceptible to dictionary attacks. | [CRYPTO\_CIPHER\_CONSTANT\_IV] Constant block cipher initialization vector [CRYPTO\_CIPHER\_NO\_IV] Missing block cipher initialization vector [CRYPTO\_CIPHER\_PREDICTABLE\_IV] Predictable block cipher initialization vector |
| [CWE-330] The software may use insufficiently random numbers or values in a security context that depends on unpredictable numbers. | [CRYPTO\_CIPHER\_PREDICTABLE\_IV] Predictable block cipher initialization vector [CRYPTO\_CIPHER\_PREDICTABLE\_KEY] Predictable cipher key [RAND\_SEED\_CONSTANT] Deterministic random output from constant seed [RAND\_SEED\_PREDICTABLE] Predictable random output from predictable seed [VULNERABLE\_PRNG] Vulnerable pseudo-random number generator |
| [CWE-336] A PRNG uses the same seed each time the product is initialized. If an attacker can guess (or knows) the seed, then he/she may be able to determine the "random" number produced from the PRNG. | [RAND\_SEED\_CONSTANT] Deterministic random output from constant seed |
| [CWE-337] A PRNG is initialized from a predictable seed, e.g. using process ID or system time. | [RAND\_SEED\_PREDICTABLE] Predictable random output from predictable seed |
| [CWE-338] The product uses a Pseudo-Random Number Generator (PRNG) in a security context, but the PRNG is not cryptographically strong. | [CRYPTO\_CIPHER\_PREDICTABLE\_IV] Predictable block cipher initialization vector [CRYPTO\_CIPHER\_PREDICTABLE\_KEY] Predictable cipher key [VULNERABLE\_PRNG] Vulnerable pseudo-random number generator |
| [CWE-353] The software uses a transmission protocol that does not include a mechanism for verifying the integrity of the data during transmission, such as a checksum. | [CRYPTO\_MD\_WEAK\_HASH] Nonsecure hash algorithm [CRYPTO\_MD\_BAD\_FUNCTION] Context initialized incorrectly for digest operation |
| [CWE-354] The software does not validate or incorrectly validates the integrity check values or "checksums" of a message. This may prevent it from detecting if the data has been modified or corrupted in transmission. | [CRYPTO\_MD\_BAD\_FUNCTION] Context initialized incorrectly for digest operation |
| [CWE-362] The program contains a code sequence that can run concurrently with other code, and the code sequence requires temporary, exclusive access to a shared resource, but a timing window exists in which the shared resource can be modified by another code sequence that is operating concurrently. | [DOUBLE\_RESOURCE\_OPEN] Opening previously opened resource [FILE\_EXPOSURE\_TO\_CHILD] File descriptor exposure to child process |
| [CWE-364] The software uses a signal handler that introduces a race condition. | [SIG\_HANDLER\_SHARED\_OBJECT] Shared data access within signal handler [SIG\_HANDLER\_ASYNC\_UNSAFE] Function called from signal handler not asynchronous-safe [SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT] Function called from signal handler not asynchronous-safe (strict ISO C) |
| [CWE-366] If two threads of execution use a resource simultaneously, there exists the possibility that resources may be used while invalid, in turn making the state of execution undefined. | [DATA\_RACE] Data race [DATA\_RACE\_ALL] Data race including atomic operations [DATA\_RACE\_STD\_LIB] Data race through standard library function call |
| [CWE-367] The software checks the state of a resource before using that resource, but the resource's state can change between the check and the use in a way that invalidates the results of the check. This can cause the software to perform invalid actions when the resource is in an unexpected state. | [TOCTOU] File access between time of check and use (TOCTOU) |
| [CWE-369] The product divides a value by zero. | [FLOAT\_STD\_LIB] Invalid use of standard library floating point routine [FLOAT\_ZERO\_DIV] Float division by zero [INT\_STD\_LIB] Invalid use of standard library integer routine [INT\_ZERO\_DIV] Integer division by zero [TAINTED\_INT\_DIVISION] Tainted division operand [TAINTED\_INT\_MOD] Tainted modulo operand |
| [CWE-372] The software does not properly determine which state it is in, causing it to assume it is in state X when in fact it is in state Y, causing it to perform incorrect operations in a security-relevant manner. | [CRYPTO\_CIPHER\_BAD\_FUNCTION] Inconsistent cipher operations [CRYPTO\_CIPHER\_NO\_DATA] Missing cipher data to process [CRYPTO\_CIPHER\_NO\_FINAL] Missing cipher final step [CRYPTO\_PKEY\_NO\_PARAMS] Missing parameters for key generation [CRYPTO\_PKEY\_NO\_DATA] Missing data for encryption, decryption or signing operation [CRYPTO\_PKEY\_INCORRECT\_INIT] Context initialized incorrectly for cryptographic operation [CRYPTO\_RSA\_BAD\_PADDING] Incompatible padding for RSA algorithm operation [CRYPTO\_MD\_BAD\_FUNCTION] Context initialized incorrectly for digest operation |
| [CWE-375] Sending non-cloned mutable data as a return value may result in that data being altered or deleted by the calling function. | [BREAKING\_DATA\_ENCAPSULATION] Return of non-const handle to encapsulated data member |
| [CWE-377] Creating and using insecure temporary files can leave application and system data vulnerable to attack. | [NON\_SECURE\_TEMP\_FILE] Use of non-secure temporary file |
| [CWE-387] Weaknesses in this category are related to the improper handling of signals. | [SIG\_HANDLER\_COMP\_EXCP\_RETURN] Return from computational exception signal handler [SIG\_HANDLER\_CALLING\_SIGNAL] Signal call from within signal handler [SIG\_HANDLER\_ASYNC\_UNSAFE] Function called from signal handler not asynchronous-safe [SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT] Function called from signal handler not asynchronous-safe (strict ISO C) |
| [CWE-391] Ignoring exceptions and other error conditions may allow an attacker to induce unexpected behavior unnoticed. | [ERRNO\_NOT\_CHECKED] Errno not checked |
| [CWE-398] The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained. | [USELESS\_WRITE] Write without a further read |
| [CWE-401] The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory. | [MEM\_LEAK] Memory leak [THREAD\_MEM\_LEAK] Thread-specific memory leak |
| [CWE-404] The program does not release or incorrectly releases a resource before it is made available for re-use. | [BAD\_DELETE] Invalid deletion of pointer [BAD\_FREE] Invalid free of pointer [MEM\_LEAK] Memory leak [THREAD\_MEM\_LEAK] Thread-specific memory leak [WIN\_MISMATCH\_DEALLOC] Mismatched alloc/dealloc functions on Windows |
| [CWE-413] The software does not lock or does not correctly lock a resource when the software must have exclusive access to the resource. | [DATA\_RACE] Data race [DATA\_RACE\_ALL] Data race including atomic operations [DATA\_RACE\_STD\_LIB] Data race through standard library function call [SIG\_HANDLER\_SHARED\_OBJECT] Shared data access within signal handler [SIG\_HANDLER\_ASYNC\_UNSAFE] Function called from signal handler not asynchronous-safe [SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT] Function called from signal handler not asynchronous-safe (strict ISO C) [DOUBLE\_RESOURCE\_OPEN] Opening previously opened resource |
| [CWE-415] The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations. | [DOUBLE\_DEALLOCATION] Deallocation of previously deallocated pointer [MISSING\_FREED\_PTR\_RESET] Missing reset of freed pointer |
| [CWE-416] Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code. | [FREED\_PTR] Use of previously freed pointer [MISSING\_FREED\_PTR\_RESET] Missing reset of freed pointer |
| [CWE-426] The application searches for critical resources using an externally-supplied search path that can point to resources that are not under the application's direct control. | [TAINTED\_PATH\_CMD] Command executed from externally controlled path [TAINTED\_PATH\_LIB] Library loaded from externally controlled path |
| [CWE-427] The product uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors. | [RELATIVE\_PATH\_CMD] Execution of a binary from a relative path can be controlled by an external actor [RELATIVE\_PATH\_LIB] Load of library from a relative path can be controlled by an external actor |
| [CWE-456] The software does not initialize critical variables, which causes the execution environment to use unexpected values. | [MISSING\_ERRNO\_RESET] Errno not reset [NON\_INIT\_MEMBER] Member not initialized in constructor [NON\_INIT\_PTR] Non-initialized pointer [NON\_INIT\_VAR] Non-initialized variable |
| [CWE-457] The code uses a variable that has not been initialized, leading to unpredictable or unintended results. | [NON\_INIT\_MEMBER] Member not initialized in constructor [NON\_INIT\_PTR] Non-initialized pointer [NON\_INIT\_VAR] Non-initialized variable |
| [CWE-465] Weaknesses in this category are related to improper handling of pointers. | [BAD\_INT\_PTR\_CAST] Unsafe conversion between pointer and integer |
| [CWE-466] A function can return a pointer to memory that is outside of the buffer that the pointer is expected to reference. | [BAD\_INT\_PTR\_CAST] Unsafe conversion between pointer and integer [OUT\_BOUND\_ARRAY] Array access out of bounds [OUT\_BOUND\_PTR] Pointer access out of bounds |
| [CWE-467] The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated. | [PTR\_SIZEOF\_MISMATCH] Wrong type used in sizeof [SIZEOF\_MISUSE] Possible misuse of sizeof |
| [CWE-468] In C and C++, one may often accidentally refer to the wrong memory due to the semantics of when math operations are implicitly scaled. | [BAD\_PTR\_SCALING] Incorrect pointer scaling |
| [CWE-469] The application subtracts one pointer from another in order to determine size, but this calculation can be incorrect if the pointers do not exist in the same memory chunk. | [PTR\_TO\_DIFF\_ARRAY] Subtraction or comparison between pointers to different arrays |
| [CWE-471] The software does not properly protect an assumed-immutable element from being modified by an attacker. | [CONSTANT\_OBJECT\_WRITE] Writing to const qualified object |
| [CWE-474] The code uses a function that has inconsistent implementations across operating systems and versions. | [OBSOLETE\_STD\_FUNC] Use of obsolete standard function [SIG\_HANDLER\_CALLING\_SIGNAL] Signal call from within signal handler |
| [CWE-475] The behavior of this function is undefined unless its control parameter is set to a specific value. | [OVERLAPPING\_COPY] Copy of overlapping memory |
| [CWE-476] A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. | [NULL\_PTR] Null pointer [TAINTED\_STRING] Tainted NULL or non-null-terminated string |
| [CWE-477] The code uses deprecated or obsolete functions, which suggests that the code has not been actively reviewed or maintained. | [OBSOLETE\_STD\_FUNC] Use of obsolete standard function |
| [CWE-478] The code does not have a default case in a switch statement, which might lead to complex logical errors and resultant weaknesses. | [MISSING\_SWITCH\_CASE] Missing case for switch condition |
| [CWE-479] The program defines a signal handler that calls a non-reentrant function. | [SIG\_HANDLER\_ASYNC\_UNSAFE] Function called from signal handler not asynchronous-safe [SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT] Function called from signal handler not asynchronous-safe (strict ISO C) |
| [CWE-480] The programmer accidentally uses the wrong operator, which changes the application logic in security-relevant ways. | [BAD\_EQUAL\_USE] Invalid use of = operator [BAD\_EQUAL\_EQUAL\_USE] Invalid use of == operator |
| [CWE-481] The code uses an operator for assignment when the intention was to perform a comparison. | [BAD\_EQUAL\_USE] Invalid use of = operator |
| [CWE-482] The code uses an operator for comparison when the intention was to perform an assignment. | [BAD\_EQUAL\_EQUAL\_USE] Invalid use of == operator |
| [CWE-483] The code does not explicitly delimit a block that is intended to contain 2 or more statements, creating a logic error. | [INCORRECT\_INDENTATION] Incorrectly indented statement [SEMICOLON\_CTRL\_STMT\_SAME\_LINE] Semicolon on the same line as an if, for or while statement |
| [CWE-484] The program omits a break statement within a switch or similar construct, causing code associated with multiple conditions to execute. This can cause problems when the programmer only intended to execute code associated with one condition. | [MISSING\_SWITCH\_BREAK] Missing break of switch case |
| [CWE-522] This weakness occurs when the application transmits or stores authentication credentials and uses an insecure method that is susceptible to unauthorized interception and/or retrieval. | [UNSAFE\_STD\_CRYPT] Unsafe standard encryption function [CRYPTO\_SSL\_WEAK\_PROTOCOL] Nonsecure SSL/TLS protocol [CRYPTO\_PKEY\_WEAK\_PARAMS] Nonsecure parameters for key generation [CRYPTO\_RSA\_LOW\_EXPONENT] Nonsecure RSA public exponent [CRYPTO\_CIPHER\_CONSTANT\_KEY] Constant cipher key [CRYPTO\_MD\_WEAK\_HASH] Nonsecure hash algorithm |
| [CWE-532] Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information. | [SENSITIVE\_DATA\_PRINT] Sensitive data printed out |
| [CWE-534] The application does not sufficiently restrict access to a log file that is used for debugging. | [SENSITIVE\_DATA\_PRINT] Sensitive data printed out |
| [CWE-535] A command shell error message indicates that there exists an unhandled exception in the web application code. In many cases, an attacker can leverage the conditions that cause these errors in order to gain unauthorized access to the system. | [SENSITIVE\_DATA\_PRINT] Sensitive data printed out |
| [CWE-547] The program uses hard-coded constants instead of symbolic names for security-critical values, which increases the likelihood of mistakes during code maintenance or security policy change. | [HARD\_CODED\_BUFFER\_SIZE] Hard-coded buffer size [HARD\_CODED\_LOOP\_BOUNDARY] Hard-coded loop boundary |
| [CWE-558] The application uses the getlogin() function in a multithreaded context, potentially causing it to return incorrect values. | [UNSAFE\_STD\_FUNC] Unsafe standard function |
| [CWE-560] The product calls umask() with an incorrect argument that is specified as if it is an argument to chmod(). | [BAD\_UMASK] Umask used with chmod-style arguments |
| [CWE-561] The software contains dead code, which can never be executed. | [DEAD\_CODE] Dead code [UNCALLED\_FUNC] Static uncalled function [UNREACHABLE] Unreachable code |
| [CWE-562] A function returns the address of a stack variable, which will cause unintended program behavior, typically in the form of a crash. | [LOCAL\_ADDR\_ESCAPE] Pointer or reference to stack variable leaving scope [PUTENV\_AUTO\_VAR] Use of automatic variable as putenv-family function argument |
| [CWE-573] The software does not follow or incorrectly follows the specifications as required by the implementation language, environment, framework, protocol, or platform. | [WRITE\_INTERNAL\_BUFFER\_RETURNED\_FROM\_STD\_FUNC] Modification of internal buffer returned from non-reentrant standard function [CRYPTO\_CIPHER\_NO\_ALGORITHM] Missing cipher algorithm [CRYPTO\_CIPHER\_NO\_KEY] Missing cipher key [CRYPTO\_PKEY\_NO\_PUBLIC\_KEY] Missing public key [CRYPTO\_PKEY\_NO\_PEER] Missing peer key [CRYPTO\_PKEY\_NO\_PRIVATE\_KEY] Missing private key [CRYPTO\_PKEY\_NO\_PARAMS] Missing parameters for key generation [CRYPTO\_PKEY\_NO\_DATA] Missing data for encryption, decryption or signing operation [CRYPTO\_PKEY\_INCORRECT\_INIT] Context initialized incorrectly for cryptographic operation [CRYPTO\_PKEY\_INCORRECT\_KEY] Incorrect key for cryptographic algorithm [CRYPTO\_RSA\_NO\_BLINDING] Missing blinding for RSA algorithm [CRYPTO\_RSA\_BAD\_PADDING] Incompatible padding for RSA algorithm operation [CRYPTO\_MD\_BAD\_FUNCTION] Context initialized incorrectly for digest operation [CRYPTO\_MD\_NO\_ALGORITHM] Missing hash algorithm [CRYPTO\_SSL\_BAD\_ROLE] TLS/SSL connection method set incorrectly [CRYPTO\_SSL\_NO\_ROLE] TLS/SSL connection method not set [CRYPTO\_MD\_NO\_FINAL] Missing final step after hashing update operation [CRYPTO\_SSL\_NO\_PRIVATE\_KEY] Missing private key for X.509 certificate |
| [CWE-587] The software sets a pointer to a specific address other than NULL or 0. | [BAD\_INT\_PTR\_CAST] Unsafe conversion between pointer and integer [FUNC\_PTR\_ABSOLUTE\_ADDR] Function pointer assigned with absolute address |
| [CWE-590] The application calls free() on a pointer to memory that was not allocated using associated heap allocation functions such as malloc(), calloc(), or realloc(). | [BAD\_FREE] Invalid free of pointer |
| [CWE-606] The product does not properly check inputs that are used for loop conditions, potentially leading to a denial of service because of excessive looping. | [TAINTED\_LOOP\_BOUNDARY] Loop bounded with tainted value |
| [CWE-628] The product calls a function, procedure, or routine with arguments that are not correctly specified, leading to always-incorrect behavior and resultant weaknesses. | [BAD\_FILE\_ACCESS\_MODE\_STATUS] Bad file access mode or status [INVALID\_VA\_LIST\_ARG] Invalid va\_list argument [OVERLAPPING\_COPY] Copy of overlapping memory [STD\_FUNC\_ARG\_MISMATCH] Standard function call with incorrect arguments [WRITE\_INTERNAL\_BUFFER\_RETURNED\_FROM\_STD\_FUNC] Modification of internal buffer returned from non-reentrant standard function |
| [CWE-663] The software calls a non-reentrant function in a concurrent context in which a competing code sequence (e.g. thread or signal handler) may have an opportunity to call the same function or otherwise influence its state. | [UNSAFE\_STD\_CRYPT] Unsafe standard encryption function [UNSAFE\_STD\_FUNC] Unsafe standard function [SIG\_HANDLER\_ASYNC\_UNSAFE] Function called from signal handler not asynchronous-safe [SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT] Function called from signal handler not asynchronous-safe (strict ISO C) |
| [CWE-664] The software does not maintain or incorrectly maintains control over a resource throughout its lifetime of creation, use, and release. | [CRYPTO\_CIPHER\_BAD\_FUNCTION] Inconsistent cipher operations [CRYPTO\_CIPHER\_NO\_DATA] Missing cipher data to process [CRYPTO\_CIPHER\_NO\_FINAL] Missing cipher final step [CRYPTO\_CIPHER\_NO\_KEY] Missing cipher key [CRYPTO\_PKEY\_NO\_PUBLIC\_KEY] Missing public key [CRYPTO\_PKEY\_NO\_PEER] Missing peer key [CRYPTO\_PKEY\_NO\_PRIVATE\_KEY] Missing private key [CRYPTO\_PKEY\_INCORRECT\_KEY] Incorrect key for cryptographic algorithm [CRYPTO\_PKEY\_INCORRECT\_INIT] Context initialized incorrectly for cryptographic operation [CRYPTO\_RSA\_BAD\_PADDING] Incompatible padding for RSA algorithm operation [CRYPTO\_MD\_BAD\_FUNCTION] Context initialized incorrectly for digest operation |
| [CWE-665] The software does not initialize or incorrectly initializes a resource, which might leave the resource in an unexpected state when it is accessed or used. | [IMPROPER\_ARRAY\_INIT] Improper array initialization [MEMSET\_INVALID\_SIZE] Use of memset with size argument zero [MEMSET\_INVALID\_VALUE] Call to memset family with unintended value [OVERLAPPING\_ASSIGN] Overlapping assignment |
| [CWE-666] The software performs an operation on a resource at the wrong phase of the resource's lifecycle, which can lead to unexpected behaviors. | [BAD\_NETWORK\_CONNECT\_ORDER] Incorrect order of network connection operations |
| [CWE-667] The software does not properly acquire a lock on a resource, or it does not properly release a lock on a resource, leading to unexpected resource state changes and behaviors. | [BAD\_LOCK] Missing unlock [DESTROY\_LOCKED] Destruction of locked mutex [BLOCKING\_WHILE\_LOCKED] Blocking operation while holding lock |
| [CWE-672] The software uses, accesses, or otherwise operates on a resource after that resource has been expired, released, or revoked. | [CLOSED\_RESOURCE\_USE] Use of previously closed resource [DOUBLE\_RESOURCE\_CLOSE] Closing previously closed resource |
| [CWE-675] The product performs the same operation on a resource two or more times, when the operation should only be applied once. | [DOUBLE\_RESOURCE\_OPEN] Opening previously opened resource |
| [CWE-676] The program invokes a potentially dangerous function that could introduce a vulnerability if it is used incorrectly, but the function can also be used safely. | [DANGEROUS\_STD\_FUNC] Use of dangerous standard function [UNSAFE\_STR\_TO\_NUMERIC] Unsafe conversion from string to numerical value |
| [CWE-681] When converting from one data type to another, such as long to integer, data can be omitted or translated in a way that produces unexpected values. If the resulting values are used in a sensitive context, then dangerous behaviors may occur. | [FLOAT\_CONV\_OVFL] Float conversion overflow [INT\_TO\_FLOAT\_PRECISION\_LOSS] Precision loss in integer to float conversion |
| [CWE-682] The software performs a calculation that generates incorrect or unintended results that are later used in security-critical decisions or resource management. | [BAD\_PLAIN\_CHAR\_USE] Use of plain char type for numeric value [BITWISE\_NEG] Bitwise operation on negative value [FLOAT\_ABSORPTION] Absorption of float operand [FLOAT\_OVFL] Float overflow [FLOAT\_STD\_LIB] Invalid use of standard library floating point routine [INT\_STD\_LIB] Invalid use of standard library integer routine [TAINTED\_INT\_MOD] Tainted modulo operand |
| [CWE-683] The software calls a function, procedure, or routine, but the caller specifies the arguments in an incorrect order, leading to resultant weaknesses. | [STRING\_FORMAT] Format string specifiers and arguments mismatch [MEMSET\_INVALID\_VALUE] Call to memset family with unintended value |
| [CWE-685] The software calls a function, procedure, or routine, but the caller specifies too many arguments, or too few arguments, which may lead to undefined behavior and resultant weaknesses. | [DECL\_MISMATCH] Declaration mismatch [STD\_FUNC\_ARG\_MISMATCH] Standard function call with incorrect arguments [STRING\_FORMAT] Format string specifiers and arguments mismatch [TOO\_MANY\_VA\_ARG\_CALLS] Too many va\_arg calls for current argument list |
| [CWE-686] The software calls a function, procedure, or routine, but the caller specifies an argument that is the wrong data type, which may lead to resultant weaknesses. | [BAD\_FILE\_ACCESS\_MODE\_STATUS] Bad file access mode or status [CONSTANT\_OBJECT\_WRITE] Writing to const qualified object [DECL\_MISMATCH] Declaration mismatch [STD\_FUNC\_ARG\_MISMATCH] Standard function call with incorrect arguments [STRING\_FORMAT] Format string specifiers and arguments mismatch [PUTENV\_AUTO\_VAR] Use of automatic variable as putenv-family function argument [VA\_ARG\_INCORRECT\_TYPE] Incorrect data type passed to va\_arg |
| [CWE-687] The software calls a function, procedure, or routine, but the caller specifies an argument that contains the wrong value, which may lead to resultant weaknesses. | [NON\_POSITIVE\_VLA\_SIZE] Variable length array with non-positive size [OVERLAPPING\_COPY] Copy of overlapping memory [STD\_FUNC\_ARG\_MISMATCH] Standard function call with incorrect arguments |
| [CWE-690] The product does not check for an error after calling a function that can return with a NULL pointer if the function fails, which leads to a resultant NULL pointer dereference. | [UNPROTECTED\_MEMORY\_ALLOCATION] Unprotected dynamic memory allocation [RETURN\_NOT\_CHECKED] Returned value of a sensitive function not checked [NULL\_PTR] Null pointer [TAINTED\_PTR] Use of tainted pointer [TAINTED\_STRING] Tainted NULL or non-null-terminated string [MEM\_STD\_LIB] Invalid use of standard library memory routine [STR\_STD\_LIB] Invalid use of standard library string routine [OTHER\_STD\_LIB] Invalid use of standard library routine [STD\_FUNC\_ARG\_MISMATCH] Standard function call with incorrect arguments |
| [CWE-691] The code does not sufficiently manage its control flow during execution, creating conditions in which the control flow can be modified in unexpected ways. | [SETJMP\_LONGJMP\_USE] Use of setjmp/longjmp |
| [CWE-693] The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. | [CRYPTO\_SSL\_WEAK\_PROTOCOL] Nonsecure SSL/TLS protocol |
| [CWE-696] The software performs multiple related behaviors, but the behaviors are performed in the wrong order in ways which may produce resultant weaknesses. | [BAD\_PRIVILEGE\_DROP\_ORDER] Bad order of dropping privileges |
| [CWE-703] The software does not properly anticipate or handle exceptional conditions that rarely occur during normal operation of the software. | [ERRNO\_MISUSE] Misuse of errno [MISSING\_ERRNO\_RESET] Errno not reset |
| [CWE-704] The software does not correctly convert an object, resource or structure from one type to a different type. | [CHAR\_EOF\_CONFUSED] Character value absorbed into EOF [CHARACTER\_MISUSE] Misuse of sign-extended character value [OBJECT\_SIZE\_MISMATCH] Wrong allocated object size for cast [PTR\_CAST] Unreliable cast of pointer [QUALIFIER\_MISMATCH] Qualifier removed in conversion [INT\_TO\_FLOAT\_PRECISION\_LOSS] Precision loss in integer to float conversion |
| [CWE-705] The software does not properly return control flow to the proper location after it has completed a task or detected an unusual condition. | [EXIT\_ABNORMAL\_HANDLER] Abnormal termination of exit handler |
| [CWE-710] The software does not follow certain coding rules for development, which can lead to resultant weaknesses or increase the severity of the associated vulnerabilities. | [BITWISE\_ARITH\_MIX] Bitwise and arithmetic operations on the same data |
| [CWE-732] The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors. | [DANGEROUS\_PERMISSIONS] Vulnerable permission assignments |
| [CWE-754] The software does not check or improperly checks for unusual or exceptional conditions that are not expected to occur frequently during day to day operation of the software. | [RETURN\_NOT\_CHECKED] Returned value of a sensitive function not checked |
| [CWE-755] The software does not handle or incorrectly handles an exceptional condition. | [EXCP\_HANDLER\_HIDDEN] Exception handler hidden by previous handler |
| [CWE-758] The software uses an API function, data structure, or other entity in a way that relies on properties that are not always guaranteed to hold for that entity. | [BAD\_INT\_PTR\_CAST] Unsafe conversion between pointer and integer [BAD\_PLAIN\_CHAR\_USE] Use of plain char type for numeric value [BITWISE\_NEG] Bitwise operation on negative value |
| [CWE-759] The software uses a one-way cryptographic hash against an input that should not be reversible, such as a password, but the software does not also use a salt as part of the input. | [CRYPTO\_MD\_NO\_SALT] Missing salt for hashing operation |
| [CWE-762] The application attempts to return a memory resource to the system, but it calls a release function that is not compatible with the function that was originally used to allocate that resource. | [BAD\_FREE] Invalid free of pointer [WIN\_MISMATCH\_DEALLOC] Mismatched alloc/dealloc functions on Windows |
| [CWE-764] The software locks a critical resource more times than intended, leading to an unexpected state in the system. | [DOUBLE\_LOCK] Double lock |
| [CWE-765] The software unlocks a critical resource more times than intended, leading to an unexpected state in the system. | [DOUBLE\_UNLOCK] Double unlock |
| [CWE-767] The software defines a public method that reads or modifies a private variable. | [BREAKING\_DATA\_ENCAPSULATION] Return of non-const handle to encapsulated data member |
| [CWE-770] The software allocates a reusable resource or group of resources on behalf of an actor without imposing any restrictions on how many resources can be allocated, in violation of the intended security policy for that actor. | [TAINTED\_VLA\_SIZE] Tainted size of variable length array |
| [CWE-772] The software does not release a resource after its effective lifetime has ended, i.e., after the resource is no longer needed. | [RESOURCE\_LEAK] Resource leak |
| [CWE-780] The software uses the RSA algorithm but does not incorporate Optimal Asymmetric Encryption Padding (OAEP), which might weaken the encryption. | [CRYPTO\_RSA\_NO\_PADDING] Missing padding for RSA algorithm [CRYPTO\_RSA\_WEAK\_PADDING] Weak padding for RSA algorithm |
| [CWE-783] The program uses an expression in which operator precedence causes incorrect logic to be used. | [OPERATOR\_PRECEDENCE] Possibly unintended evaluation of expression because of operator precedence rules |
| [CWE-785] The software invokes a function for normalizing paths or file names, but it provides an output buffer that is smaller than the maximum possible size, such as PATH\_MAX. | [PATH\_BUFFER\_OVERFLOW] Use of path manipulation function without maximum-sized buffer checking |
| [CWE-786] The software reads or writes to a buffer using an index or pointer that references a memory location prior to the beginning of the buffer. | [STRLIB\_BUFFER\_UNDERFLOW] Destination buffer underflow in string manipulation |
| [CWE-787] The software writes data past the end, or before the beginning, of the intended buffer. | [STRLIB\_BUFFER\_OVERFLOW] Destination buffer overflow in string manipulation [STRLIB\_BUFFER\_UNDERFLOW] Destination buffer underflow in string manipulation |
| [CWE-789] The product allocates memory based on an untrusted size value, but it does not validate or incorrectly validates the size, allowing arbitrary amounts of memory to be allocated. | [TAINTED\_MEMORY\_ALLOC\_SIZE] Memory allocation with tainted size [TAINTED\_VLA\_SIZE] Tainted size of variable length array [UNPROTECTED\_MEMORY\_ALLOCATION] Unprotected dynamic memory allocation |
| [CWE-805] The software uses a sequential operation to read or write a buffer, but it uses an incorrect length value that causes it to access memory that is outside of the bounds of the buffer. | [HARD\_CODED\_MEM\_SIZE] Hard-coded object size used to manipulate memory |
| [CWE-822] The program obtains a value from an untrusted source, converts this value to a pointer, and dereferences the resulting pointer. | [TAINTED\_PTR] Use of tainted pointer [TAINTED\_STRING] Tainted NULL or non-null-terminated string |
| [CWE-823] The program performs pointer arithmetic on a valid pointer, but it uses an offset that can point outside of the intended range of valid memory locations for the resulting pointer. | [OUT\_BOUND\_PTR] Pointer access out of bounds [TAINTED\_PTR\_OFFSET] Pointer dereference with tainted offset |
| [CWE-824] The program accesses or uses a pointer that has not been initialized. | [NON\_INIT\_PTR] Non-initialized pointer |
| [CWE-825] The program dereferences a pointer that contains a location for memory that was previously valid, but is no longer valid. | [DOUBLE\_DEALLOCATION] Deallocation of previously deallocated pointer [FREED\_PTR] Use of previously freed pointer [LOCAL\_ADDR\_ESCAPE] Pointer or reference to stack variable leaving scope [TEMP\_OBJECT\_ACCESS] Accessing object with temporary lifetime [INVALID\_ENV\_POINTER] Environment pointer invalidated by previous operation [PUTENV\_AUTO\_VAR] Use of automatic variable as putenv-family function argument [MISSING\_FREED\_PTR\_RESET] Missing reset of freed pointer |
| [CWE-826] The program releases a resource that is still intended to be used by the program itself or another actor. | [DESTROY\_LOCKED] Destruction of locked mutex [CLOSED\_RESOURCE\_USE] Use of previously closed resource [DOUBLE\_RESOURCE\_CLOSE] Closing previously closed resource |
| [CWE-828] The software defines a signal handler that contains code sequences that are not asynchronous-safe, i.e., the functionality is not reentrant, or it can be interrupted. | [SIG\_HANDLER\_ASYNC\_UNSAFE] Function called from signal handler not asynchronous-safe [SIG\_HANDLER\_ASYNC\_UNSAFE\_STRICT] Function called from signal handler not asynchronous-safe (strict ISO C) |
| [CWE-832] The software attempts to unlock a resource that is not locked. | [BAD\_UNLOCK] Missing lock |
| [CWE-833] The software contains multiple threads or executable segments that are waiting for each other to release a necessary lock, resulting in deadlock. | [DEADLOCK] Deadlock |
| [CWE-843] The program allocates or initializes a resource such as a pointer, object, or variable using one type, but it later accesses that resource using a type that is incompatible with the original type. | [PTR\_CAST] Unreliable cast of pointer |
| [CWE-872] Weaknesses in this category are related to rules in the Integers (INT) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete. | [INT\_STD\_LIB] Invalid use of standard library integer routine |
| [CWE-873] Weaknesses in this category are related to rules in the Floating Point Arithmetic (FLP) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete. | [BAD\_FLOAT\_OP] Floating point comparison with equality operators [FLOAT\_ABSORPTION] Absorption of float operand [FLOAT\_OVFL] Float overflow [FLOAT\_STD\_LIB] Invalid use of standard library floating point routine |
| [CWE-908] The software uses a resource that has not been properly initialized. | [NON\_INIT\_MEMBER] Member not initialized in constructor [NON\_INIT\_PTR] Non-initialized pointer [NON\_INIT\_VAR] Non-initialized variable |
| [CWE-910] The software uses or accesses a file descriptor after it has been closed. | [CLOSED\_RESOURCE\_USE] Use of previously closed resource [DOUBLE\_RESOURCE\_CLOSE] Closing previously closed resource [STD\_FUNC\_ARG\_MISMATCH] Standard function call with incorrect arguments |
| [CWE-922] The software stores sensitive information without properly limiting read or write access by unauthorized actors. | [BAD\_UMASK] Umask used with chmod-style arguments [CHROOT\_MISUSE] File manipulation after chroot() without chdir("/") [DANGEROUS\_PERMISSIONS] Vulnerable permission assignments [NON\_SECURE\_TEMP\_FILE] Use of non-secure temporary file |

Files with compilation errors (files partially analyzed)

Table 3.2. Files with compilation errors (files partially analyzed)

|  |
| --- |
| **File** |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_134.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_176.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_469.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_483.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_561.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_588.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_670.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\CWE\_672.c |
| D:\polyspace\_yanglimin\194 C Code\hou\CWE C Code\MAIN.c |

Chapter 4. Appendix 2 - Definitions

Table 4.1. Abbreviations

|  |  |
| --- | --- |
| **Abbreviation** | **Definition** |
| NA | Not Available |