vul_files_51 Scan Report

Project Name	vul_files_51
Scan Start	Wednesday, January 8, 2025 12:12:40 PM
Preset	Checkmarx Default
Scan Time	03h:47m:01s
Lines Of Code Scanned	297670
Files Scanned	54
Report Creation Time	Wednesday, January 8, 2025 3:08:05 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	5/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None
OWASP Top 10 2013	None
FISMA 2014	None

NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None

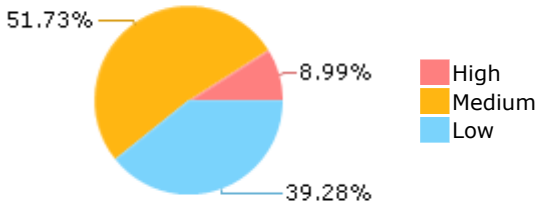
Results Limit

Results limit per query was set to 50

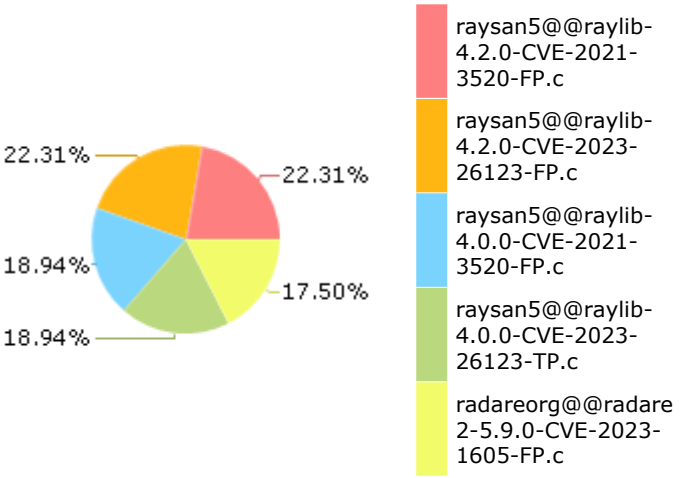
Selected Queries

Selected queries are listed in Result Summary

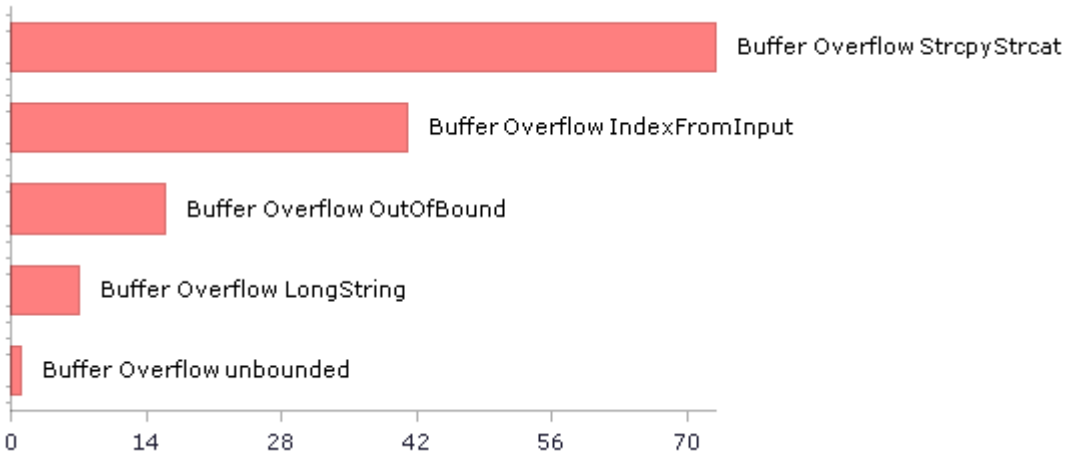
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2017

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	277	194
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	82	82
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	23	23
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	1	1
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	308	308
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: OWASP Top 10 2013

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	1	1
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	308	308
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

* Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	4	4
PCI DSS (3.2) - 6.5.2 - Buffer overflows	183	136
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	13	13
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	69	69
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	23	23
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	3	3

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	82	82
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	23	23
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	349	242
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	283	235
SI-11 Error Handling (P2)*	226	226
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	8	8

***** Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

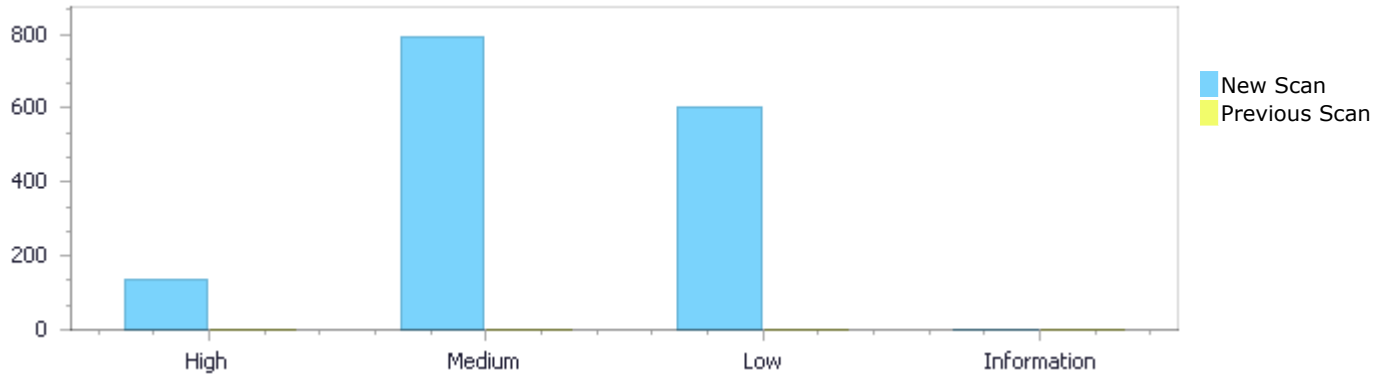
Scan Summary - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	138	794	603	0	1,535
Recurrent Issues	0	0	0	0	0
Total	138	794	603	0	1,535
Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	138	794	603	0	1,535
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	138	794	603	0	1,535

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	73	High
Buffer Overflow IndexFromInput	41	High
Buffer Overflow OutOfBound	16	High
Buffer Overflow LongString	7	High
Buffer Overflow unbounded	1	High

Dangerous Functions	308	Medium
Memory Leak	186	Medium
Use of Zero Initialized Pointer	146	Medium
Buffer Overflow boundcpy WrongSizeParam	79	Medium
MemoryFree on StackVariable	53	Medium
Divide By Zero	7	Medium
Double Free	4	Medium
Integer Overflow	3	Medium
Buffer Overflow AddressOfLocalVarReturned	2	Medium
Char Overflow	2	Medium
Stored Buffer Overflow boundcpy	2	Medium
Wrong Memory Allocation	1	Medium
Wrong Size t Allocation	1	Medium
Unchecked Return Value	226	Low
Unchecked Array Index	141	Low
Improper Resource Access Authorization	69	Low
Potential Precision Problem	37	Low
Use of Sizeof On a Pointer Type	34	Low
TOCTOU	33	Low
Use of Insufficiently Random Values	23	Low
NULL Pointer Dereference	15	Low
Incorrect Permission Assignment For Critical Resources	13	Low
Sizeof Pointer Argument	7	Low
Potential Off by One Error in Loops	4	Low
Potential Path Traversal	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	74
raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	74
raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	68
raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	61
raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	61
raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	60
raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	60
raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	60
radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	60
radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c	56

Scan Results Details

Buffer Overflow StrcpyStrcat

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow StrcpyStrcat Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=9
Status	New

The size of the buffer used by createAnonymousFile in path, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that createAnonymousFile passes to getenv, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	111	119
Object	getenv	path

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static int createAnonymousFile(off_t size)

```
....
111.          path = getenv("XDG_RUNTIME_DIR");
....
119.          strcpy(name, path);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=10
Status	New

The size of the buffer used by createAnonymousFile in name, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that createAnonymousFile passes to getenv, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	111	120
Object	getenv	name

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static int createAnonymousFile(off_t size)

```
....
111.          path = getenv("XDG_RUNTIME_DIR");
....
120.          strcat(name, template);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=11
Status New

The size of the buffer used by createAnonymousFile in name, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that createAnonymousFile passes to getenv, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	111	119
Object	getenv	name

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static int createAnonymousFile(off_t size)

```
....
111.          path = getenv("XDG_RUNTIME_DIR");
....
119.          strcpy(name, path);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=12
Status	New

The size of the buffer used by TakeScreenshot in fileName, at line 1807 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 1807 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1807	1816
Object	fileName	fileName

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method void TakeScreenshot(const char *fileName)

```
....
1807.  void TakeScreenshot(const char *fileName)
....
1816.      strcat(path, fileName);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=13
Status	New

The size of the buffer used by IsFileExtension in fileExt, at line 1849 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 1849 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1849	1860
Object	fileName	fileExt

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
1849.  bool IsFileExtension(const char *fileName, const char *ext)
....
1860.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=14
Status	New

The size of the buffer used by IsFileExtension in TextToLower, at line 1849 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 1849 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1849	1860
Object	fileName	TextToLower

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
1849.  bool IsFileExtension(const char *fileName, const char *ext)
....
1860.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=15
Status	New

The size of the buffer used by *GetFileNameWithoutExt in filePath, at line 1920 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 1920 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1920	1927
Object	filePath	filePath

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
1920.  const char *GetFileNameWithoutExt(const char *filePath)
....
1927.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=16
Status	New

The size of the buffer used by *GetFileNameWithoutExt in GetFileName, at line 1920 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 1920 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1920	1927
Object	filePath	GetFileName

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
1920.  const char *GetFileNameWithoutExt(const char *filePath)
....
1927.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=17
Status	New

The size of the buffer used by **GetDirectoryFiles in d_name, at line 2011 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2011 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Line	2011	2033
Object	dirPath	d_name

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2011.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2033.              strcpy(dirFilesPath[counter], ent->d_name);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=18
Status	New

The size of the buffer used by **GetDirectoryFiles in dirFilesPath, at line 2011 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2011 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2011	2033
Object	dirPath	dirFilesPath

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2011.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2033.              strcpy(dirFilesPath[counter], ent->d_name);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=19
Status	New

The size of the buffer used by WindowDropCallback in paths, at line 4067 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WindowDropCallback passes to paths, at line 4067 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4067	4076
Object	paths	paths

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
4067.  static void WindowDropCallback(GLFWwindow *window, int count,
const char **paths)
....
4076.          strcpy(dropFilesPath[i], paths[i]);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=20
Status New

The size of the buffer used by TakeScreenshot in fileName, at line 2168 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 2168 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2168	2177
Object	fileName	fileName

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method void TakeScreenshot(const char *fileName)

```
....
2168.  void TakeScreenshot(const char *fileName)
....
2177.      strcat(path, fileName);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=21

Status	New

The size of the buffer used by IsFileExtension in fileExt, at line 2228 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2228 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2228	2240
Object	fileName	fileExt

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2228.  bool IsFileExtension(const char *fileName, const char *ext)
....
2240.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=22
Status	New

The size of the buffer used by IsFileExtension in TextToLower, at line 2228 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2228 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2228	2240
Object	fileName	TextToLower

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2228.  bool IsFileExtension(const char *fileName, const char *ext)
....
2240.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=23
Status	New

The size of the buffer used by *GetFileNameWithoutExt in filePath, at line 2303 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2303 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2303	2310
Object	filePath	filePath

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2303.  const char *GetFileNameWithoutExt(const char *filePath)
....
2310.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=24
Status	New

The size of the buffer used by *GetFileNameWithoutExt in GetFileName, at line 2303 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2303 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2303	2310
Object	filePath	GetFileName

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2303.  const char *GetFileNameWithoutExt(const char *filePath)
....
2310.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=25
Status	New

The size of the buffer used by **GetDirectoryFiles in d_name, at line 2401 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2401 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2401	2423
Object	dirPath	d_name

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2401.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2423.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=26
Status	New

The size of the buffer used by **GetDirectoryFiles in dirFilesPath, at line 2401 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2401 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2401	2423

Object	dirPath	dirFilesPath

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2401.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2423.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=27
Status	New

The size of the buffer used by WindowDropCallback in paths, at line 4713 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WindowDropCallback passes to paths, at line 4713 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4713	4722
Object	paths	paths

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
4713.  static void WindowDropCallback(GLFWwindow *window, int count,
const char **paths)
....
4722.          strcpy(CORE.Window.dropFilesPath[i], paths[i]);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=28
Status	New

The size of the buffer used by TakeScreenshot in fileName, at line 2168 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that TakeScreenshot passes to fileName, at line 2168 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2168	2177
Object	fileName	fileName

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method void TakeScreenshot(const char *fileName)

```
....
2168.  void TakeScreenshot(const char *fileName)
....
2177.      strcat(path, fileName);
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=29
Status New

The size of the buffer used by IsFileExtension in fileExt, at line 2228 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2228 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2228	2240
Object	fileName	fileExt

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2228.  bool IsFileExtension(const char *fileName, const char *ext)
....
2240.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=30
Status	New

The size of the buffer used by IsFileExtension in TextToLower, at line 2228 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2228 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2228	2240
Object	fileName	TextToLower

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2228.  bool IsFileExtension(const char *fileName, const char *ext)
....
2240.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=31
Status	New

The size of the buffer used by *GetFileNameWithoutExt in filePath, at line 2303 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2303 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2303	2310
Object	filePath	filePath

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2303.  const char *GetFileNameWithoutExt(const char *filePath)
....
2310.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=32
Status	New

The size of the buffer used by *GetFileNameWithoutExt in GetFileName, at line 2303 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2303 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2303	2310
Object	filePath	GetFileName

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2303.  const char *GetFileNameWithoutExt(const char *filePath)
....
2310.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=33
Status	New

The size of the buffer used by **GetDirectoryFiles in d_name, at line 2401 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2401 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2401	2423
Object	dirPath	d_name

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2401.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2423.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=34
Status	New

The size of the buffer used by **GetDirectoryFiles in dirFilesPath, at line 2401 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2401 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2401	2423
Object	dirPath	dirFilesPath

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2401.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2423.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=35
Status	New

The size of the buffer used by WindowDropCallback in paths, at line 4713 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WindowDropCallback passes to paths, at line 4713 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4713	4722
Object	paths	paths

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
4713.  static void WindowDropCallback(GLFWwindow *window, int count,
const char **paths)
....
4722.          strcpy(CORE.Window.dropFilesPath[i], paths[i]);
```

Buffer Overflow StrcpyStrcat\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=36
Status	New

The size of the buffer used by TakeScreenshot in fileName, at line 2662 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 2662 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2662	2668
Object	fileName	fileName

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void TakeScreenshot(const char *fileName)

```
....
2662.  void TakeScreenshot(const char *fileName)
....
2668.      strcpy(path, TextFormat("%s/%s", CORE.Storage.basePath,
fileName));
```

Buffer Overflow StrcpyStrcat\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=37
Status	New

The size of the buffer used by TakeScreenshot in TextFormat, at line 2662 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 2662 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2662	2668
Object	fileName	TextFormat

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void TakeScreenshot(const char *fileName)

```
....
2662.  void TakeScreenshot(const char *fileName)
....
2668.      strcpy(path, TextFormat("%s/%s", CORE.Storage.basePath,
fileName));
```

Buffer Overflow StrcpyStrcat\Path 30:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=38
Status New

The size of the buffer used by IsFileExtension in fileExt, at line 2717 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2717 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2717	2729
Object	fileName	fileExt

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2717.  bool IsFileExtension(const char *fileName, const char *ext)
....
2729.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 31:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=39
Status New

The size of the buffer used by IsFileExtension in TextToLower, at line 2717 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2717 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2717	2729
Object	fileName	TextToLower

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2717.  bool IsFileExtension(const char *fileName, const char *ext)
....
2729.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=40
Status	New

The size of the buffer used by *GetFileNameWithoutExt in filePath, at line 2792 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2792 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2792	2799
Object	filePath	filePath

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2792.  const char *GetFileNameWithoutExt(const char *filePath)
....
2799.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=41
Status	New

The size of the buffer used by *GetFileNameWithoutExt in GetFileName, at line 2792 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2792 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2792	2799
Object	filePath	GetFileName

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2792.  const char *GetFileNameWithoutExt(const char *filePath)
....
2799.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=42
Status	New

The size of the buffer used by **GetDirectoryFiles in d_name, at line 2899 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2899 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2899	2921
Object	dirPath	d_name

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2899.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2921.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=43
Status	New

The size of the buffer used by **GetDirectoryFiles in dirFilesPath, at line 2899 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2899 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2899	2921
Object	dirPath	dirFilesPath

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2899.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2921.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=44
Status	New

The size of the buffer used by WindowDropCallback in paths, at line 5241 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WindowDropCallback passes to paths, at line 5241 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5241	5250
Object	paths	paths

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
5241.  static void WindowDropCallback(GLFWwindow *window, int count,
const char **paths)
....
5250.          strcpy(CORE.Window.dropFilesPath[i], paths[i]);
```

Buffer Overflow StrcpyStrcat\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=45
Status	New

The size of the buffer used by TakeScreenshot in fileName, at line 2662 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 2662 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2662	2668
Object	fileName	fileName

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method	void TakeScreenshot(const char *fileName)

```
....
2662.  void TakeScreenshot(const char *fileName)
....
2668.      strcpy(path, TextFormat("%s/%s", CORE.Storage.basePath,
fileName));
```

Buffer Overflow StrcpyStrcat\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=46
Status	New

The size of the buffer used by TakeScreenshot in TextFormat, at line 2662 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 2662 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2662	2668
Object	fileName	TextFormat

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method void TakeScreenshot(const char *fileName)

```
....
2662.  void TakeScreenshot(const char *fileName)
....
2668.      strcpy(path, TextFormat("%s/%s", CORE.Storage.basePath,
fileName));
```

Buffer Overflow StrcpyStrcat\Path 39:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=47
Status New

The size of the buffer used by IsFileExtension in fileExt, at line 2717 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2717 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2717	2729
Object	fileName	fileExt

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2717.  bool IsFileExtension(const char *fileName, const char *ext)
....
2729.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 40:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=48
Status New

The size of the buffer used by IsFileExtension in TextToLower, at line 2717 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that IsFileExtension passes to fileName, at line 2717 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2717	2729
Object	fileName	TextToLower

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method bool IsFileExtension(const char *fileName, const char *ext)

```
....
2717.  bool IsFileExtension(const char *fileName, const char *ext)
....
2729.          strcpy(fileExtLower, TextToLower(fileExt));
```

Buffer Overflow StrcpyStrcat\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=49
Status	New

The size of the buffer used by *GetFileNameWithoutExt in filePath, at line 2792 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2792 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2792	2799
Object	filePath	filePath

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2792.  const char *GetFileNameWithoutExt(const char *filePath)
....
2799.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=50
Status	New

The size of the buffer used by *GetFileNameWithoutExt in GetFileName, at line 2792 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2792 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2792	2799
Object	filePath	GetFileName

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2792.  const char *GetFileNameWithoutExt(const char *filePath)
....
2799.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=51
Status	New

The size of the buffer used by **GetDirectoryFiles in d_name, at line 2899 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2899 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2899	2921
Object	dirPath	d_name

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2899.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2921.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=52
Status	New

The size of the buffer used by **GetDirectoryFiles in dirFilesPath, at line 2899 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that **GetDirectoryFiles passes to dirPath, at line 2899 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2899	2921
Object	dirPath	dirFilesPath

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2899.  char **GetDirectoryFiles(const char *dirPath, int *fileCount)
....
2921.              strcpy(dirFilesPath[counter], entity->d_name);
```

Buffer Overflow StrcpyStrcat\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=53
Status	New

The size of the buffer used by WindowDropCallback in paths, at line 5241 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that WindowDropCallback passes to paths, at line 5241 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	5241	5250
Object	paths	paths

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
5241.  static void WindowDropCallback(GLFWwindow *window, int count,
const char **paths)
....
5250.          strcpy(CORE.Window.dropFilesPath[i], paths[i]);
```

Buffer Overflow StrcpyStrcat\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=54
Status	New

The size of the buffer used by TakeScreenshot in fileName, at line 2767 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that TakeScreenshot passes to fileName, at line 2767 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2767	2775
Object	fileName	fileName

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void TakeScreenshot(const char *fileName)

```
....
2767.  void TakeScreenshot(const char *fileName)
....
2775.      strcpy(path, TextFormat("%s/%s", CORE.Storage.basePath,
fileName));
```

Buffer Overflow StrcpyStrcat\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=55
Status	New

The size of the buffer used by *GetFileNameWithoutExt in filePath, at line 2927 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2927 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2927	2934
Object	filePath	filePath

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2927.  const char *GetFileNameWithoutExt(const char *filePath)
....
2934.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 48:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=56
Status New

The size of the buffer used by *GetFileNameWithoutExt in GetFileName, at line 2927 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GetFileNameWithoutExt passes to filePath, at line 2927 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2927	2934
Object	filePath	GetFileName

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method const char *GetFileNameWithoutExt(const char *filePath)

```
....
2927.  const char *GetFileNameWithoutExt(const char *filePath)
....
2934.      if (filePath != NULL) strcpy(fileName,
GetFileName(filePath));   // Get filename with extension
```

Buffer Overflow StrcpyStrcat\Path 49:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=57

Status	New

The size of the buffer used by ScanDirectoryFiles in path, at line 5113 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ScanDirectoryFiles passes to basePath, at line 5113 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5113	5134
Object	basePath	path

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ScanDirectoryFiles(const char *basePath, FilePathList *files, const char *filter)

```
....
5113.  static void ScanDirectoryFiles(const char *basePath, FilePathList
*files, const char *filter)
....
5134.                           strcpy(files->paths[files->count], path);
```

Buffer Overflow StrcpyStrcat\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=58
Status	New

The size of the buffer used by ScanDirectoryFiles in paths, at line 5113 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ScanDirectoryFiles passes to basePath, at line 5113 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5113	5134
Object	basePath	paths

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ScanDirectoryFiles(const char *basePath, FilePathList *files, const char *filter)

```
....
5113.  static void ScanDirectoryFiles(const char *basePath, FilePathList
*files, const char *filter)
....
5134.                           strcpy(files->paths[files->count], path);
```

Buffer Overflow IndexFromInput

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow IndexFromInput Version:1

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=82
Status	New

The size of the buffer used by vorbis_finish_frame in i, at line 3456 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get8 passes to fgetc, at line 1337 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	3474
Object	fgetc	i

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method static int vorbis_finish_frame(stb_vorbis *f, int len, int left, int right)

```
....
3474.             f->channel_buffers[i][left+j] =
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=83
Status	New

The size of the buffer used by vorbis_finish_frame in i, at line 3456 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get8 passes to fgetc, at line 1337 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	3493
Object	fgetc	i

Code Snippet

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method static int vorbis_finish_frame(stb_vorbis *f, int len, int left, int right)

```
....
3493.           f->previous_window[i][j] = f-
>channel_buffers[i][right+j];
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=84
Status	New

The size of the buffer used by vorbis_decode_packet_rest in blockflag, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get8 passes to fgetc, at line 1337 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	3190
Object	fgetc	blockflag

Code Snippet

File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3190.     n = f->blocksize[m->blockflag];
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=85
Status	New

The size of the buffer used by vorbis_decode_packet_rest in mapping, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get8 passes to fgetc, at line 1337 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	3191
Object	fgetc	mapping

Code Snippet

File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3191.     map = &f->mapping[m->mapping];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=86
Status	New

The size of the buffer used by crc32_update in BinaryExpr, at line 1003 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get8 passes to fgetc, at line 1337 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	1005
Object	fgetc	BinaryExpr

Code Snippet

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method static __forceinline uint32 crc32_update(uint32 crc, uint8 byte)

```
....
1005.     return (crc << 8) ^ crc_table[byte ^ (crc >> 24)];
```

Buffer Overflow IndexFromInput\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=87
Status	New

The size of the buffer used by *GamepadThread in i, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5133	5145
Object	Address	i

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5133.               if (read(gamepadStream[i], &gamepadEvent,
sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5145.
currentGamepadState[i][gamepadEvent.number] = (int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=88
Status	New

The size of the buffer used by *GamepadThread in i, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5133	5158
Object	Address	i

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5133.               if (read(gamepadStream[i], &gamepadEvent,
sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5158.                           gamepadAxisState[i][gamepadEvent.number]
= (float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=89
Status	New

The size of the buffer used by *GamepadThread in number, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5133	5145
Object	Address	number

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5133.               if (read(gamepadStream[i], &gamepadEvent,
sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5145.
currentGamepadState[i][gamepadEvent.number] = (int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 9:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=90
Status New

The size of the buffer used by *GamepadThread in number, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5133	5158
Object	Address	number

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5133.               if (read(gamepadStream[i], &gamepadEvent,
sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5158.                           gamepadAxisState[i][gamepadEvent.number]
= (float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 10:

Severity High
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=91
Status	New

The size of the buffer used by *EventThread in BinaryExpr, at line 4864 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *EventThread passes to Address, at line 4864 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4896	4996
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
4896.           if (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
....
4996.                       keycode = keymap_US[event.code & 0xFF];
// The code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=92
Status	New

The size of the buffer used by *EventThread in BinaryExpr, at line 5538 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *EventThread passes to Address, at line 5538 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5570	5669
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *EventThread(void *arg)

```
....
5570.          while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
....
5669.                        keycode = keymap_US[event.code & 0xFF];
// The code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=93
Status	New

The size of the buffer used by *GamepadThread in i, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5797	5809
Object	Address	i

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5809.
CORE.Input.Gamepad.currentState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=94
Status	New

The size of the buffer used by *GamepadThread in i, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination

File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5797	5822
Object	Address	i

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5822.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=95
Status New

The size of the buffer used by *GamepadThread in number, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5797	5809
Object	Address	number

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5809.
CORE.Input.Gamepad.currentState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=96
Status	New

The size of the buffer used by *GamepadThread in number, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5797	5822
Object	Address	number

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5822.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=97
Status	New

The size of the buffer used by *EventThread in BinaryExpr, at line 5538 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *EventThread passes to Address, at line 5538 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5570	5669
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
5570.          while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
....
5669.                        keycode = keymap_US[event.code & 0xFF];
// The code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=98
Status	New

The size of the buffer used by *GamepadThread in i, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5797	5809
Object	Address	i

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5809.
CORE.Input.Gamepad.currentState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=99
Status	New

The size of the buffer used by *GamepadThread in i, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

Source	Destination

File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5797	5822
Object	Address	i

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5822.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 19:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=100
Status New

The size of the buffer used by *GamepadThread in number, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5797	5809
Object	Address	number

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5809.
CORE.Input.Gamepad.currentState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 20:

Severity High
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=101
Status	New

The size of the buffer used by *GamepadThread in number, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 5777 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5797	5822
Object	Address	number

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
5822.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=102
Status	New

The size of the buffer used by PollKeyboardEvents in BinaryExpr, at line 5982 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PollKeyboardEvents passes to Address, at line 5982 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6012	6024
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void PollKeyboardEvents(void)

```
....
6012.      while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
....
6024.                  keycode = keymapUS[event.code & 0xFF];     // The
code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=103
Status	New

The size of the buffer used by *GamepadThread in i, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6282	6294
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6282.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6294.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=104
Status	New

The size of the buffer used by *GamepadThread in number, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-	raysan5@@raylib-4.0.0-CVE-2021-3520-

	FP.c	FP.c
Line	6282	6294
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6294.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=105
Status	New

The size of the buffer used by *GamepadThread in i, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6282	6307
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6307.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=106
Status	New

The size of the buffer used by *GamepadThread in number, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6282	6307
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6307.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=107
Status	New

The size of the buffer used by PollKeyboardEvents in BinaryExpr, at line 5982 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PollKeyboardEvents passes to Address, at line 5982 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6012	6024
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void PollKeyboardEvents(void)

```
....
6012.      while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
....
6024.                  keycode = keymapUS[event.code & 0xFF];     // The
code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=108
Status	New

The size of the buffer used by *GamepadThread in i, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6282	6294
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void *GamepadThread(void *arg)

```
....
6282.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6294.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=109
Status	New

The size of the buffer used by *GamepadThread in number, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-	raysan5@@raylib-4.0.0-CVE-2023-

	26123-TP.c	26123-TP.c
Line	6282	6294
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6294.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=110
Status	New

The size of the buffer used by *GamepadThread in i, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6282	6307
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6307.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=111
Status	New

The size of the buffer used by *GamepadThread in number, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6262 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6282	6307
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6307.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=112
Status	New

The size of the buffer used by PollKeyboardEvents in BinaryExpr, at line 6250 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PollKeyboardEvents passes to Address, at line 6250 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6280	6292
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void PollKeyboardEvents(void)

```
....
6280.       while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
....
6292.                       keycode = keymapUS[event.code & 0xFF];      // The
code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=113
Status	New

The size of the buffer used by *GamepadThread in i, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6550	6562
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6562.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=114
Status	New

The size of the buffer used by *GamepadThread in number, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-	raysan5@@raylib-4.2.0-CVE-2021-3520-

	FP.c	FP.c
Line	6550	6562
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6562.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=115
Status	New

The size of the buffer used by *GamepadThread in i, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6550	6575
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6575.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=116
Status	New

The size of the buffer used by *GamepadThread in number, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6550	6575
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6575.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=117
Status	New

The size of the buffer used by PollKeyboardEvents in BinaryExpr, at line 6250 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that PollKeyboardEvents passes to Address, at line 6250 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6280	6292
Object	Address	BinaryExpr

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void PollKeyboardEvents(void)

```
....
6280.      while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
....
6292.                  keycode = keymapUS[event.code & 0xFF];     // The
code we get is a scancode so we look up the apropriate keycode
```

Buffer Overflow IndexFromInput\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=118
Status	New

The size of the buffer used by *GamepadThread in i, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6550	6562
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6562.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=119
Status	New

The size of the buffer used by *GamepadThread in number, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-	raysan5@@raylib-4.2.0-CVE-2023-

	26123-FP.c	26123-FP.c
Line	6550	6562
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6562.
CORE.Input.Gamepad.currentButtonState[i][gamepadEvent.number] =
(int)gamepadEvent.value;
```

Buffer Overflow IndexFromInput\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=120
Status	New

The size of the buffer used by *GamepadThread in i, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6550	6575
Object	Address	i

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6575.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=121
Status	New

The size of the buffer used by *GamepadThread in number, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *GamepadThread passes to Address, at line 6530 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6550	6575
Object	Address	number

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
....
6575.
CORE.Input.Gamepad.axisState[i][gamepadEvent.number] =
(float)gamepadEvent.value/32768;
```

Buffer Overflow IndexFromInput\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=122
Status	New

The size of the buffer used by readDataOfferAsString in length, at line 953 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that readDataOfferAsString passes to BinaryExpr, at line 953 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	991	1011
Object	BinaryExpr	length

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static char* readDataOfferAsString(struct wl_data_offer* offer, const char* mimeType)

```
....
991.          const ssize_t result = read(fds[0], string + length,
readSize);
....
1011.      string[length] = '\0';
```

Buffer Overflow OutOfBound

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow OutOfBound Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=123
Status	New

The size of the buffer used by main in y, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Line	34	39
Object	colorsRecs	y

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
39.          colorsRecs[i].y = 10;
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=124
Status	New

The size of the buffer used by main in x, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Line	34	38
Object	colorsRecs	x

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
38.          colorsRecs[i].x = 10 + 30*i + 2*i;
```

Buffer Overflow OutOfBound\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=125
Status New

The size of the buffer used by main in width, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Line	34	40
Object	colorsRecs	width

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
40.          colorsRecs[i].width = 30;
```

Buffer Overflow OutOfBound\Path 4:

Severity High
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=126
Status	New

The size of the buffer used by main in height, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Line	34	41
Object	colorsRecs	height

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24805-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
41.          colorsRecs[i].height = 30;
```

Buffer Overflow OutOfBound\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=127
Status	New

The size of the buffer used by main in y, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Line	34	39
Object	colorsRecs	y

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
39.          colorsRecs[i].y = 10;
```

Buffer Overflow OutOfBound\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=128
Status	New

The size of the buffer used by main in x, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Line	34	38
Object	colorsRecs	x

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
38.          colorsRecs[i].x = 10 + 30*i + 2*i;
```

Buffer Overflow OutOfBound\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=129
Status	New

The size of the buffer used by main in width, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Line	34	40
Object	colorsRecs	width

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Method	int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
40.          colorsRecs[i].width = 30;
```

Buffer Overflow OutOfBound\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=130
Status	New

The size of the buffer used by main in height, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Line	34	41
Object	colorsRecs	height

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2022-24807-FP.c
Method	int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
41.          colorsRecs[i].height = 30;
```

Buffer Overflow OutOfBound\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=131
Status	New

The size of the buffer used by main in y, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-	raysan5@@raylib-2.6.0-CVE-2022-

	24808-FP.c	24808-FP.c
Line	34	39
Object	colorsRecs	y

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
39.          colorsRecs[i].y = 10;
```

Buffer Overflow OutOfBound\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=132
Status	New

The size of the buffer used by main in x, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Line	34	38
Object	colorsRecs	x

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
38.          colorsRecs[i].x = 10 + 30*i + 2*i;
```

Buffer Overflow OutOfBound\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=133
Status	New

The size of the buffer used by main in width, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Line	34	40
Object	colorsRecs	width

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
40.          colorsRecs[i].width = 30;
```

Buffer Overflow OutOfBound\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=134
Status New

The size of the buffer used by main in height, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to colorsRecs, at line 18 of raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c	raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Line	34	41
Object	colorsRecs	height

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-24808-FP.c
Method int main(void)

```
....
34.      Rectangle colorsRecs[MAX_COLORS_COUNT] = { 0 };
....
41.          colorsRecs[i].height = 30;
```

Buffer Overflow OutOfBound\Path 13:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=135
Status	New

The size of the buffer used by *GamepadThread in i, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that descriptor passes to gamepadStream, at line 425 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	425	5133
Object	gamepadStream	i

Code Snippet

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Method static int gamepadStream[MAX_GAMEPADS] = { -1 };// Gamepad device file descriptor

```
....
425.  static int gamepadStream[MAX_GAMEPADS] = { -1 };// Gamepad device
file descriptor
```

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Method static void *GamepadThread(void *arg)

```
....
5133.              if (read(gamepadStream[i], &gamepadEvent,
sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Buffer Overflow OutOfBound\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=136
Status	New

The size of the buffer used by *GamepadThread in currentGamepadState, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that state passes to currentGamepadState, at line 421 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	421	5145
Object	currentGamepadState	currentGamepadState

Code Snippet

File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static char currentGamepadState[MAX_GAMEPADS][MAX_GAMEPAD_BUTTONS]; // Current gamepad buttons state

```
....
421.  static char
currentGamepadState[MAX_GAMEPADS][MAX_GAMEPAD_BUTTONS];     // Current
gamepad buttons state
```

File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static void *GamepadThread(void *arg)

```
....
5145.
currentGamepadState[i][gamepadEvent.number] = (int)gamepadEvent.value;
```

Buffer Overflow OutOfBound\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=137
Status	New

The size of the buffer used by *GamepadThread in currentGamepadState, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that state passes to gamepadAxisState, at line 419 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	419	5145
Object	gamepadAxisState	currentGamepadState

Code Snippet

File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static float gamepadAxisState[MAX_GAMEPADS][MAX_GAMEPAD_AXIS]; // Gamepad axis state

```
....
419.  static float gamepadAxisState[MAX_GAMEPADS][MAX_GAMEPAD_AXIS];  //
Gamepad axis state
```

File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static void *GamepadThread(void *arg)

```
....
5145.
currentGamepadState[i][gamepadEvent.number] = (int)gamepadEvent.value;
```

Buffer Overflow OutOfBound\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=138
Status	New

The size of the buffer used by *GamepadThread in gamepadAxisState, at line 5113 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that state passes to gamepadAxisState, at line 419 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	419	5158
Object	gamepadAxisState	gamepadAxisState

Code Snippet

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Method static float gamepadAxisState[MAX_GAMEPADS][MAX_GAMEPAD_AXIS]; // Gamepad axis state

```
....
419.  static float gamepadAxisState[MAX_GAMEPADS][MAX_GAMEPAD_AXIS];  //
Gamepad axis state
```

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Method static void *GamepadThread(void *arg)

```
....
5158.                          gamepadAxisState[i][gamepadEvent.number]
= (float)gamepadEvent.value/32768;
```

Buffer Overflow LongString

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow LongString Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1
Status	New

The size of the buffer used by _glfwDetectJoystickConnectionWin32 in guid, at line 496 of raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwDetectJoystickConnectionWin32 passes to "78696e707574%02x00000000000000000", at line 496 of raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	526	529
Object	"78696e707574%02x0000000000000000"	guid

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method void _glfwDetectJoystickConnectionWin32(void)

```
....
526.              sprintf(guid, "78696e707574%02x00000000000000000",
....
529.              js = _glfwAllocJoystick(getDeviceDescription(&xic),
guid, 6, 10, 1);
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=2
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to "mt.__newindex = function (t, n, v)\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	883	883
Object	"mt.__newindex = function (t, n, v)\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c

Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
883.      s[j++]="mt.__newindex = function (t, n, v)\n";
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=3
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " local w = dbg.getinfo(2, \"S\").what\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	885	885
Object	" local w = dbg.getinfo(2, \"S\").what\n"	s

Code Snippet	
File Name	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method	void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
885.      s[j++]="    local w = dbg.getinfo(2, \"S\").what\n";
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=4
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if w ~= \"main\" and w ~= \"C\" then\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	886	886
Object	" if w ~= \"main\" and w ~= \"C\"	s

	then\n"	

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
886.      s[j++]="    if w ~= \"main\" and w ~= \"C\" then\n";
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=5
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	887	887
Object	" error(\"Script attempted to create global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
887.      s[j++]="      error(\"Script attempted to create global
variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=6
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	893	893
Object	" if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~= \"C\" then\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
893.      s[j++]="  if dbg.getinfo(2) and dbg.getinfo(2, \"S\").what ~=
\"C\" then\n";
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=7
Status	New

The size of the buffer used by scriptingEnableGlobalsProtection in s, at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that scriptingEnableGlobalsProtection passes to " error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n", at line 873 of redis@@redis-5.0.10-CVE-2021-32626-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	894	894
Object	" error(\"Script attempted to access nonexistent global variable '\"..tostring(n)..\"'\", 2)\n"	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method void scriptingEnableGlobalsProtection(lua_State *lua) {

```
....
894.      s[j++]="    error(\"Script attempted to access nonexistent
global variable '\"..tostring(n)..\"'\", 2)\n";
```

Buffer Overflow unbounded

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow unbounded Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow unbounded\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=8
Status	New

The size of the buffer used by createAnonymousFile in path, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that createAnonymousFile passes to getenv, at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	111	119
Object	getenv	path

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static int createAnonymousFile(off_t size)

```
....
111.          path = getenv("XDG_RUNTIME_DIR");
....
119.          strcpy(name, path);
```

Dangerous Functions

Query Path:
CPP\Cx\CPP Medium Threat\Dangerous Functions Version:1

Categories

OWASP Top 10 2013: A9-Using Components with Known Vulnerabilities
OWASP Top 10 2017: A9-Using Components with Known Vulnerabilities

Description

Dangerous Functions\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=633
Status	New

The dangerous function, memcpy, was found in use at line 745 in radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	781	781
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *copy_object(pyc_object *object) {

```
....
781.                    memcpy (dst, src, sizeof (*dst));
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=634
Status	New

The dangerous function, memcpy, was found in use at line 315 in radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Line	330	330
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Method struct r_bin_te_section_t* r_bin_te_get_sections(struct r_bin_te_obj_t* bin) {

```
....
330.              memcpy (sections[i].name, shdr[i].Name,
TE_IMAGE_SIZEOF_NAME);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=635
Status	New

The dangerous function, memcpy, was found in use at line 70 in radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Line	106	106
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Method static bool r_debug_qnx_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
106.        memcpy ((void *)(volatile void *) buf, pd->desc->recv.data,
copy_size);
```

Dangerous Functions\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=636
Status New

The dangerous function, memcpy, was found in use at line 70 in radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Line	108	108
Object	memcpy	memcpy

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Method static bool r_debug_qnx_reg_read(RDebug *dbg, int type, ut8 *buf, int size) {

```
....
108.        memcpy ((void *)(volatile void *) pd->reg_buf, pd->desc-
>recv.data, copy_size);
```

Dangerous Functions\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=637
Status	New

The dangerous function, memcpy, was found in use at line 136 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	148	148
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
148.            memcpy(disconnected,
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=638
Status	New

The dangerous function, memcpy, was found in use at line 477 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	488	488
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
488.        memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=639
Status	New

The dangerous function, memcpy, was found in use at line 477 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	489	489
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
489.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=640
Status	New

The dangerous function, memcpy, was found in use at line 477 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	490	490
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
490.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=641
Status	New

The dangerous function, memcpy, was found in use at line 495 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	507	507
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
507.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=642
Status	New

The dangerous function, memcpy, was found in use at line 495 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	508	508
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
508.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=643
Status	New

The dangerous function, memcpy, was found in use at line 495 in raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	509	509
Object	memcpy	memcpy

Code Snippet

File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c

Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
509.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=644
Status	New

The dangerous function, memcpy, was found in use at line 2328 in raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2357	2357
Object	memcpy	memcpy

Code Snippet

File Name	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method	const char *GetDirectoryPath(const char *filePath)

```
....
2357.           memcpy(dirPath + ((filePath[1] != ':')? 2 : 0), filePath,
strlen(filePath) - (strlen(lastSlash) - 1));
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=645
Status	New

The dangerous function, memcpy, was found in use at line 137 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	149	149
Object	memcpy	memcpy

Code Snippet

File Name	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method	void _glfwPollMonitorsWin32(void)

```
....
149.           memcpy(disconnected,
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=646
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	491	491
Object	memcpy	memcpy

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method	GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=647
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	492	492
Object	memcpy	memcpy

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method	GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=648
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c

Line	493	493
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=649
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	510	510
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=650
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	511	511
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Dangerous Functions\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=651
Status New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	512	512
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Dangerous Functions\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=652
Status New

The dangerous function, memcpy, was found in use at line 2328 in raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2357	2357
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2357.           memcpy(dirPath + ((filePath[1] != ':')? 2 : 0), filePath,
strlen(filePath) - (strlen(lastSlash) - 1));
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=653
Status	New

The dangerous function, memcpy, was found in use at line 137 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	149	149
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
149.           memcpy(disconnected,
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=654

Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	491	491
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=655
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	492	492
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=656
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	493	493
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=657
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	510	510
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=658
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	511	511
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=659
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	512	512
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=660
Status	New

The dangerous function, memcpy, was found in use at line 2817 in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2854	2854
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2854.              memcpy(dirPath + (filePath[1] != ':' && filePath[0]
!= '\\' && filePath[0] != '/' ? 2 : 0), filePath, strlen(filePath) -
(strlen(lastSlash) - 1));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=661
Status	New

The dangerous function, memcpy, was found in use at line 137 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	149	149
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
149.          memcpy(disconnected,
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=662
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	491	491
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=663
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	492	492

Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=664
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	493	493
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=665
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	510	510
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=666
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	511	511
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=667
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	512	512
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=668
Status New

The dangerous function, memcpy, was found in use at line 2817 in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2854	2854
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2854.              memcpy(dirPath + (filePath[1] != ':' && filePath[0]
!= '\\' && filePath[0] != '/' ? 2 : 0), filePath, strlen(filePath) -
(strlen(lastSlash) - 1));
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=669
Status	New

The dangerous function, memcpy, was found in use at line 2952 in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2989	2989
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2989.               memcpy(dirPath + (filePath[1] != ':' && filePath[0]
!= '\\' && filePath[0] != '/' ? 2 : 0), filePath, strlen(filePath) -
(strlen(lastSlash) - 1));
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=670
Status	New

The dangerous function, memcpy, was found in use at line 137 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	149	149
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
149.           memcpy(disconnected,
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=671
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	491	491
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=672
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	492	492
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=673
Status	New

The dangerous function, memcpy, was found in use at line 480 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	493	493
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=674
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	510	510
Object	memcpy	memcpy

Code Snippet

File Name	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method	void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=675
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	511	511
Object	memcpy	memcpy

Code Snippet

File Name	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method	void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=676
Status	New

The dangerous function, memcpy, was found in use at line 498 in raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	512	512

Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=677
Status	New

The dangerous function, memcpy, was found in use at line 2952 in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2989	2989
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2989.              memcpy(dirPath + (filePath[1] != ':' && filePath[0]
!= '\\' && filePath[0] != '/' ? 2 : 0), filePath, strlen(filePath) -
(strlen(lastSlash) - 1));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=678
Status	New

The dangerous function, memcpy, was found in use at line 5453 in raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5465	5465
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method int stb_vorbis_get_samples_float(stb_vorbis *f, int channels, float **buffer, int num_samples)

```
....
5465.              memcpy(buffer[i]+n, f->channel_buffers[i]+f-
>channel_buffer_start, sizeof(float)*k);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=679
Status	New

The dangerous function, memcpy, was found in use at line 1363 in raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1367	1367
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int getn(vorb *z, uint8 *data, int n)

```
....
1367.         memcpy(data, z->stream, n);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=680
Status	New

The dangerous function, memcpy, was found in use at line 3180 in raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3296	3296
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3296.     memcpy(really_zero_channel, zero_channel,
sizeof(really_zero_channel[0]) * f->channels);
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=681
Status New

The dangerous function, memcpy, was found in use at line 3580 in raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3779	3779
Object	memcpy	memcpy

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3779.           memcpy(c->codeword_lengths, lengths, c->entries);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=682
Status New

The dangerous function, memcpy, was found in use at line 89 in redis@@redis-5.0.10-CVE-2021-21309-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-21309-TP.c	redis@@redis-5.0.10-CVE-2021-21309-TP.c
Line	142	142
Object	memcpy	memcpy

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-21309-TP.c
Method sds sdsnewlen(const void *init, size_t initlen) {

```
....
142.          memcpy(s, init, initlen);
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=945
Status New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	290	290
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
290.                    res->name = __resource_type_str (ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 2:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=946
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	290	290
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method static bool __ne_get_resources(r_bin_ne_obj_t *bin) {

```
....
290.                    res->name = __resource_type_str (ti.rtTypeID &
~0x8000);
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=947
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1289	1289
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int init_blocksize(vorb *f, int b, int n)

```
....
1289.     f->A[b] = (float *) setup_malloc(f, sizeof(float) * n2);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=948
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1290	1290
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int init_blocksize(vorb *f, int b, int n)

```
....
1290.     f->B[b] = (float *) setup_malloc(f, sizeof(float) * n2);
```

Memory Leak\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=949
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1291	1291
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int init_blocksize(vorb *f, int b, int n)

```
....
1291.     f->C[b] = (float *) setup_malloc(f, sizeof(float) * n4);
```

Memory Leak\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=950
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1294	1294

Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int init_blocksize(vorb *f, int b, int n)

```
....
1294.     f->window[b] = (float *) setup_malloc(f, sizeof(float) * n2);
```

Memory Leak\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=951
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1297	1297
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int init_blocksize(vorb *f, int b, int n)

```
....
1297.     f->bit_reverse[b] = (uint16 *) setup_malloc(f, sizeof(uint16)
* n8);
```

Memory Leak\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=952
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3653	3653
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3653.     f->vendor = (char*)setup_malloc(f, sizeof(char) * (len+1));
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=953
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3664	3664
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3664.         f->comment_list = (char**) setup_malloc(f, sizeof(char*) *
(f->comment_list_length));
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=954
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3670	3670
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3670.         f->comment_list[i] = (char*)setup_malloc(f, sizeof(char) *
(len+1));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=955
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3716	3716
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3716.     f->codebooks = (Codebook *) setup_malloc(f, sizeof(*f->codebooks) * f->codebook_count);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=956
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3742	3742
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3742.           lengths = c->codeword_lengths = (uint8 *) setup_malloc(f, c->entries);
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=957
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3777	3777
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3777.           c->codeword_lengths = (uint8 *) setup_malloc(f, c-
>entries);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=958
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3807	3807
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3807.               c->codeword_lengths = (uint8 *) setup_malloc(f, c-
>sorted_entries);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=959
Status	New

	Source	Destination

File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3826	3826
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3826.           c->sorted_codewords = (uint32 *) setup_malloc(f,
sizeof(*c->sorted_codewords) * (c->sorted_entries+1));
```

Memory Leak\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=960
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3830	3830
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3830.           c->sorted_values    = ( int   *) setup_malloc(f,
sizeof(*c->sorted_values   ) * (c->sorted_entries+1));
```

Memory Leak\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=961
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3937	3937

Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3937.     f->floor_config = (Floor *)  setup_malloc(f, f->floor_count *
sizeof(*f->floor_config));
```

Memory Leak\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=962
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4049	4049
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
4049.         r->classdata = (uint8 **) setup_malloc(f, sizeof(*r-
>classdata) * f->codebooks[r->classbook].entries);
```

Memory Leak\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=963
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4065	4065
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method	static int start_decoder(vorb *f)

```
....
4065.      f->mapping = (Mapping *) setup_malloc(f, f->mapping_count *
sizeof(*f->mapping));
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=964
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4072	4072
Object	setup_malloc	setup_malloc

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int start_decoder(vorb *f)

```
....
4072.         m->chan = (MappingChannel *) setup_malloc(f, f->channels *
sizeof(*m->chan));
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=965
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4132	4132
Object	setup_malloc	setup_malloc

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int start_decoder(vorb *f)

```
....
4132.        f->channel_buffers[i] = (float *) setup_malloc(f,
sizeof(float) * f->blocksize_1);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=966
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4133	4133
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
4133.        f->previous_window[i] = (float *) setup_malloc(f,
sizeof(float) * f->blocksize_1/2);
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=967
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4134	4134
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
4134.        f->finalY[i]          = (int16 *) setup_malloc(f,
sizeof(int16) * longest_floorlist);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=968
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4138	4138
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
4138.         f->floor_buffers[i]   = (float *) setup_malloc(f,
sizeof(float) * f->blocksize_1/2);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=969
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4335	4335
Object	setup_malloc	setup_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static stb_vorbis * vorbis_alloc(stb_vorbis *f)

```
....
4335.     stb_vorbis *p = (stb_vorbis *) setup_malloc(f, sizeof(*p));
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=970
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2118	2118
Object	setup_temp_malloc	setup_temp_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2118.     uint8 ***part_classdata = (uint8 ***) temp_block_array(f,f->channels, part_read * sizeof(**part_classdata));
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=971
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2635	2635
Object	setup_temp_malloc	setup_temp_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void inverse_mdct(float *buffer, int n, vorb *f, int blocktype)

```
....
2635.     float *buf2 = (float *) temp_alloc(f, n2 * sizeof(*buf2));
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=972
Status	New

	Source	Destination

File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3740	3740
Object	setup_temp_malloc	setup_temp_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3740.           lengths = (uint8 *) setup_temp_malloc(f, c->entries);
```

Memory Leak\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=973
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3809	3809
Object	setup_temp_malloc	setup_temp_malloc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3809.              c->codewords = (uint32 *) setup_temp_malloc(f,
sizeof(*c->codewords) * c->sorted_entries);
```

Memory Leak\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=974
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3811	3811
Object	setup_temp_malloc	setup_temp_malloc

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int start_decoder(vorb *f)

```
....
3811.              values = (uint32 *) setup_temp_malloc(f,
sizeof(*values) * c->sorted_entries);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=975
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3863	3863
Object	setup_temp_malloc	setup_temp_malloc

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int start_decoder(vorb *f)

```
....
3863.           mults = (uint16 *) setup_temp_malloc(f, sizeof(mults[0])
* c->lookup_values);
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=976
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	283	283
Object	s	s

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method	static pyc_object *get_float_object(RBuffer *buffer) {

```
....
283.        ut8 *s = malloc (n + 1);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=977
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	343	343
Object	s1	s1

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
343.        ut8 *s1 = malloc (n1 + 1);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=978
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	365	365
Object	s2	s2

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
365.        ut8 *s2 = malloc (n2 + 1);
```

Memory Leak\Path 35:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=979
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	42	42
Object	str	str

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.   char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=980
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	132	132
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
132.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=981
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	338	338
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
338.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=982
Status New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	42	42
Object	str	str

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method static char *__read_nonnull_str_at(RBuffer *buf, ut64 offset) {

```
....
42.   char *str = malloc ((ut64)sz + 1);
```

Memory Leak\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=983
Status New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	132	132

Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_symbols(r_bin_ne_obj_t *bin) {

```
....
132.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=984
Status New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	338	338
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_imports(r_bin_ne_obj_t *bin) {

```
....
338.              char *name = malloc ((ut64)sz + 1);
```

Memory Leak\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=985
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1879	1879
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method bool DirectoryExists(const char *dirPath)

```
....
1879.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=986
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2023	2023
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2023.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=987
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2262	2262
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method bool DirectoryExists(const char *dirPath)

```
....
2262.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 44:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=988
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2413	2413
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2413.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=989
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2262	2262
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method bool DirectoryExists(const char *dirPath)

```
....
2262.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=990
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2413	2413
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2413.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=991
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2751	2751
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method bool DirectoryExists(const char *dirPath)

```
....
2751.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=992
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2911	2911

Object	dir	dir

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2911.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=993
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2751	2751
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method bool DirectoryExists(const char *dirPath)

```
....
2751.       DIR *dir = opendir(dirPath);
```

Memory Leak\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=994
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2911	2911
Object	dir	dir

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2911.       DIR *dir = opendir(dirPath);
```

Use of Zero Initialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1131
Status	New

The variable declared in current at radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c in line 116 is not initialized when it is used by current at radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c in line 116.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Line	147	149
Object	current	current

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Method static bool r_debug_qnx_reg_write(RDebug *dbg, int type, const ut8 *buf, int size) {

```
....
147.        RRegItem *current = NULL;
....
149.              current = r_reg_next_diff (dbg->reg, type, pd->reg_buf, buflen, current, bits);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1132
Status	New

The variable declared in sect at radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c in line 89 is not initialized when it is used by sect at radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c in line 89.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Line	90	114
Object	sect	sect

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Method static RList *sections(RBinFile *bf) {

```
....
90.   xbe_section *sect = NULL;
....
114.        sect = calloc (h->sections, sizeof (xbe_section));
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1133
Status New

The variable declared in result at raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c in line 383 is not initialized when it is used by result at raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c in line 383.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	386	442
Object	result	result

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method GLFWvidmode* _glfwPlatformGetVideoModes(_GLFWmonitor* monitor, int* count)

```
....
386.      GLFWvidmode* result = NULL;
....
442.              result = (GLFWvidmode*) realloc(result, size *
sizeof(GLFWvidmode));
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1134
Status New

The variable declared in latestMatch at raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c in line 1901 is not initialized when it is used by latestMatch at raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c in line 1901.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1903	1904
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
1903.       const char *latestMatch = NULL;
1904.       for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1135
Status New

The variable declared in latestMatch at raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c in line 1901 is not initialized when it is used by fileName at raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c in line 1909.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1903	1912
Object	latestMatch	fileName

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
1903.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method const char *GetFileName(const char *filePath)

```
....
1912.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1136
Status	New

The variable declared in latestMatch at raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c in line 1901 is not initialized when it is used by lastSlash at raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c in line 1945.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1903	1965
Object	latestMatch	lastSlash

Code Snippet

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Method static const char *strprbrk(const char *s, const char *charset)

```
....
1903.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Method const char *GetDirectoryPath(const char *filePath)

```
....
1965.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1137
Status	New

The variable declared in latestMatch at raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c in line 2284 is not initialized when it is used by latestMatch at raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c in line 2284.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c

Line	2286	2287
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2286.       const char *latestMatch = NULL;
2287.       for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1138
Status New

The variable declared in latestMatch at raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c in line 2284 is not initialized when it is used by fileName at raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c in line 2292.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2286	2295
Object	latestMatch	fileName

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2286.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method const char *GetFileName(const char *filePath)

```
....
2295.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1139

Status	New

The variable declared in latestMatch at raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c in line 2284 is not initialized when it is used by lastSlash at raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c in line 2328.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2286	2353
Object	latestMatch	lastSlash

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2286.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2353.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1140
Status	New

The variable declared in result at raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c in line 386 is not initialized when it is used by result at raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c in line 386.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	389	445
Object	result	result

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method GLFWvidmode* _glfwPlatformGetVideoModes(_GLFWmonitor* monitor, int* count)

```
....
389.      GLFWvidmode* result = NULL;
....
445.              result = (GLFWvidmode*) realloc(result, size *
sizeof(GLFWvidmode));
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1141
Status	New

The variable declared in latestMatch at raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c in line 2284 is not initialized when it is used by latestMatch at raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c in line 2284.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2286	2287
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2286.      const char *latestMatch = NULL;
2287.      for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1142
Status	New

The variable declared in latestMatch at raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c in line 2284 is not initialized when it is used by fileName at raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c in line 2292.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2286	2295
Object	latestMatch	fileName

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2286.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c

Method const char *GetFileName(const char *filePath)

```
....
2295.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1143
Status	New

The variable declared in latestMatch at raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c in line 2284 is not initialized when it is used by lastSlash at raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c in line 2328.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2286	2353
Object	latestMatch	lastSlash

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2286.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c

Method const char *GetDirectoryPath(const char *filePath)

```
....
2353.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1144
Status	New

The variable declared in result at raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c in line 386 is not initialized when it is used by result at raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c in line 386.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	389	445
Object	result	result

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWvidmode* _glfwPlatformGetVideoModes(_GLFWmonitor* monitor, int* count)

```
....
389.      GLFWvidmode* result = NULL;
....
445.              result = (GLFWvidmode*) realloc(result, size *
sizeof(GLFWvidmode));
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1145
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c in line 2773 is not initialized when it is used by latestMatch at raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c in line 2773.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2775	2776
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2775.      const char *latestMatch = NULL;
2776.      for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1146
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c in line 2773 is not initialized when it is used by fileName at raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c in line 2781.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2775	2784
Object	latestMatch	fileName

Code Snippet

File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c

Method static const char *strprbrk(const char *s, const char *charset)

```
....
2775.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c

Method const char *GetFileName(const char *filePath)

```
....
2784.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1147
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c in line 2773 is not initialized when it is used by lastSlash at raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c in line 2817.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2775	2842
Object	latestMatch	lastSlash

Code Snippet

File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static const char *strprbrk(const char *s, const char *charset)

```
....
2775.       const char *latestMatch = NULL;
```

File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	const char *GetDirectoryPath(const char *filePath)

```
....
2842.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1148
Status	New

The variable declared in result at raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c in line 386 is not initialized when it is used by result at raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c in line 386.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	389	445
Object	result	result

Code Snippet

File Name	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method	GLFWvidmode* _glfwPlatformGetVideoModes(_GLFWmonitor* monitor, int* count)

```
....
389.       GLFWvidmode* result = NULL;
....
445.               result = (GLFWvidmode*) realloc(result, size *
sizeof(GLFWvidmode));
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1149
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c in line 2773 is not initialized when it is used by latestMatch at raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c in line 2773.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2775	2776
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2775.       const char *latestMatch = NULL;
2776.       for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1150
Status New

The variable declared in latestMatch at raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c in line 2773 is not initialized when it is used by fileName at raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c in line 2781.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2775	2784
Object	latestMatch	fileName

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2775.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method const char *GetFileName(const char *filePath)

```
....
2784.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 21:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1151
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c in line 2773 is not initialized when it is used by lastSlash at raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c in line 2817.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2775	2842
Object	latestMatch	lastSlash

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2775.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2842.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1152
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 2908 is not initialized when it is used by latestMatch at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 2908.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2910	2911
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2910.       const char *latestMatch = NULL;
2911.       for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1153
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 2908 is not initialized when it is used by fileName at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 2916.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2910	2919
Object	latestMatch	fileName

Code Snippet

File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c

Method static const char *strprbrk(const char *s, const char *charset)

```
....
2910.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c

Method const char *GetFileName(const char *filePath)

```
....
2919.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1154
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 2908 is not initialized when it is used by lastSlash at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 2952.

	Source	Destination

File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2910	2977
Object	latestMatch	lastSlash

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2910.       const char *latestMatch = NULL;
```

File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method const char *GetDirectoryPath(const char *filePath)

```
....
2977.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1155
Status	New

The variable declared in result at raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c in line 386 is not initialized when it is used by result at raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c in line 386.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	389	445
Object	result	result

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWvidmode* _glfwPlatformGetVideoModes(_GLFWmonitor* monitor, int* count)

```
....
389.       GLFWvidmode* result = NULL;
....
445.               result = (GLFWvidmode*) realloc(result, size *
sizeof(GLFWvidmode));
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1156
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 2908 is not initialized when it is used by latestMatch at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 2908.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2910	2911
Object	latestMatch	latestMatch

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2910.       const char *latestMatch = NULL;
2911.       for (; s = strpbrk(s, charset), s != NULL; latestMatch = s++)
{ }
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1157
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 2908 is not initialized when it is used by fileName at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 2916.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2910	2919
Object	latestMatch	fileName

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static const char *strprbrk(const char *s, const char *charset)

```
....
2910.       const char *latestMatch = NULL;
```

File Name	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method	const char *GetFileName(const char *filePath)

```
....
2919.       if (filePath != NULL) fileName = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1158
Status	New

The variable declared in latestMatch at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 2908 is not initialized when it is used by lastSlash at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 2952.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2910	2977
Object	latestMatch	lastSlash

Code Snippet

File Name	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method	static const char *strprbrk(const char *s, const char *charset)

```
....
2910.       const char *latestMatch = NULL;
```

File Name	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method	const char *GetDirectoryPath(const char *filePath)

```
....
2977.       lastSlash = strprbrk(filePath, "\\/");
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1159
Status	New

The variable declared in string at raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c in line 953 is not initialized when it is used by string at raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c in line 953.

	Source	Destination

File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	969	987
Object	string	string

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static char* readDataOfferAsString(struct wl_data_offer* offer, const char* mimeType)

```
....
969.      char* string = NULL;
....
987.              string = longer;
```

Use of Zero Initialized Pointer\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1160
Status New

The variable declared in keysyms at raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c in line 2264 is not initialized when it is used by keysyms at raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c in line 2264.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	2286	2299
Object	keysyms	keysyms

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method const char* _glfwGetScancodeNameWayland(int scancode)

```
....
2286.      const xkb_keysym_t* keysyms = NULL;
....
2299.      const uint32_t codepoint = _glfwKeySym2Unicode(keysyms[0]);
```

Use of Zero Initialized Pointer\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1161
Status New

The variable declared in defaultCursorHiDPI at raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c in line 2576 is not initialized when it is used by defaultCursorHiDPI at raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c in line 2576.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	2628	2638
Object	defaultCursorHiDPI	defaultCursorHiDPI

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method void _glfwSetCursorWayland(_GLFWwindow* window, _GLFWcursor* cursor)

```
....
2628.               struct wl_cursor* defaultCursorHiDPI = NULL;
....
2638.                   defaultCursorHiDPI,
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1162
Status New

The variable declared in vector at redis@@redis-5.0.10-CVE-2021-21309-TP.c in line 955 is not initialized when it is used by vector at redis@@redis-5.0.10-CVE-2021-21309-TP.c in line 955.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-21309-TP.c	redis@@redis-5.0.10-CVE-2021-21309-TP.c
Line	958	1045
Object	vector	vector

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-21309-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
958.      char **vector = NULL;
....
1045.             vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Zero Initialized Pointer\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=1163
Status	New

The variable declared in vector at redis@@redis-5.0.10-CVE-2021-21309-TP.c in line 955 is not initialized when it is used by vector at redis@@redis-5.0.10-CVE-2021-21309-TP.c in line 955.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-21309-TP.c	redis@@redis-5.0.10-CVE-2021-21309-TP.c
Line	958	1058
Object	vector	vector

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-21309-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
958.        char **vector = NULL;
....
1058.           sdsfree(vector[*argc]);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1164
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	355	433
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.        static robj **argv = NULL;
....
433.                decrRefCount(argv[j]);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1165
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by cached_objects at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	355	631
Object	argv	cached_objects

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
631.              cached_objects[j] = o;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1166
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	355	468
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1167
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	355	448
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
448.      argv = c->argv;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1168
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	355	468
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
468.      cmd = lookupCommand(argv[0]->ptr);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1169
Status	New

The variable declared in argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348 is not initialized when it is used by argv at redis@@redis-5.0.10-CVE-2021-32626-TP.c in line 348.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	355	392
Object	argv	argv

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
355.      static robj **argv = NULL;
....
392.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1170
Status	New

The variable declared in endptr at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by cg at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1129	1870
Object	endptr	cg

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.       char *endptr = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xgroupCommand(client *c) {

```
....
1870.           cg->last_id = id;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1171
Status	New

The variable declared in lp at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	549	711
Object	lp	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
549.       si->lp = NULL; /* There is no current listpack right now. */
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.       si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=1172
Status	New

The variable declared in lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	550	711
Object	lp_ele	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
550.      si->lp_ele = NULL; /* Current listpack cursor. */
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1173
Status	New

The variable declared in lp at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 557 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	616	711
Object	lp	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method int streamIteratorGetID(streamIterator *si, streamID *id, int64_t *numfields) {

```
....
616.                        si->lp = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1174
Status	New

The variable declared in endptr at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1129	711
Object	endptr	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.      char *endptr = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.      si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=1175
Status	New

The variable declared in BinaryExpr at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1396	711
Object	BinaryExpr	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xreadCommand(client *c) {

```
....
1396.       streamCG **groups = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
711.       si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1176
Status	New

The variable declared in lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	550	708
Object	lp_ele	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
550.      si->lp_ele = NULL; /* Current listpack cursor. */
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1177
Status	New

The variable declared in lp at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 512 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	549	708
Object	lp	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorStart(streamIterator *si, stream *s, streamID *start, streamID *end, int rev) {

```
....
549.      si->lp = NULL; /* There is no current listpack right now. */
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1178
Status	New

The variable declared in lp at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 557 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	616	708
Object	lp	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method int streamIteratorGetID(streamIterator *si, streamID *id, int64_t *numfields) {

```
....
616.                        si->lp = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1179
Status	New

The variable declared in endptr at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1121 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1129	708
Object	endptr	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method int string2ull(const char *s, unsigned long long *value) {

```
....
1129.       char *endptr = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1180
Status	New

The variable declared in BinaryExpr at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1387 is not initialized when it is used by lp_ele at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 702.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1396	708
Object	BinaryExpr	lp_ele

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xreadCommand(client *c) {

```
....
1396.       streamCG **groups = NULL;
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void streamIteratorGetField(streamIterator *si, unsigned char **fieldptr, unsigned char **valueptr, int64_t *fieldlen, int64_t *valuelen) {

```
....
708.          si->lp_ele = lpNext(si->lp,si->lp_ele);
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:

CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=436
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 477 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 477 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	488	488
Object	values	values

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
488.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=437
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 477 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 477 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	489	489
Object	values	values

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c

Method	GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
489.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=438
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 477 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 477 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	490	490
Object	values	values

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method	GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
490.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=439
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 495 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 495 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	507	507
Object	values	values

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method	void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
507.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=440
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 495 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 495 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	508	508
Object	values	values

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method	void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
508.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=441
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 495 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 495 of raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c

Line	509	509
Object	values	values

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
509.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=442
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	491	491
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=443
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	492	492
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=444
Status New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	493	493
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=445
Status New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	510	510
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=446
Status New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	511	511
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=447
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	512	512
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=448
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	491	491
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=449
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	492	492
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=450
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	493	493
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=451
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	510	510
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=452
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	511	511
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=453
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	512	512
Object	values	values

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=454
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	491	491
Object	values	values

Code Snippet

File Name	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method	GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=455
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	492	492
Object	values	values

Code Snippet

File Name	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method	GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=456
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	493	493

Object	values	values

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=457
Status New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	510	510
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=458
Status New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination

File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	511	511
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=459
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	512	512
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=460
Status	New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	491	491
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
491.      memcpy(ramp->red,   values[0], sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=461
Status New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	492	492
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
492.      memcpy(ramp->green, values[1], sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=462
Status New

The size of the buffer used by _glfwPlatformGetGammaRamp in values, at line 480 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformGetGammaRamp passes to values, at line 480 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	493	493
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method GLFWbool _glfwPlatformGetGammaRamp(_GLFWmonitor* monitor, GLFWgammaramp* ramp)

```
....
493.      memcpy(ramp->blue,  values[2], sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=463
Status New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	510	510
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
510.      memcpy(values[0], ramp->red,   sizeof(values[0]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=464
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	511	511
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
511.      memcpy(values[1], ramp->green, sizeof(values[1]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=465
Status	New

The size of the buffer used by _glfwPlatformSetGammaRamp in values, at line 498 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _glfwPlatformSetGammaRamp passes to values, at line 498 of raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	512	512
Object	values	values

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPlatformSetGammaRamp(_GLFWmonitor* monitor, const GLFWgammaramp* ramp)

```
....
512.      memcpy(values[2], ramp->blue,  sizeof(values[2]));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=466
Status	New

The size of the buffer used by streamEncodeID in e, at line 156 of redis@@redis-5.0.10-CVE-2021-32628-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that streamEncodeID passes to e, at line 156 of redis@@redis-5.0.10-CVE-2021-32628-TP.c, to overwrite the target buffer.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	160	160
Object	e	e

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method void streamEncodeID(void *buf, streamID *id) {

```
....
160.      memcpy(buf,e,sizeof(e));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=467
Status	New

The size of the buffer used by EventThreadSpawn in InputEventWorker, at line 4668 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EventThreadSpawn passes to InputEventWorker, at line 4668 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4706	4706
Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void EventThreadSpawn(char *device)

```
....
4706.          memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=468
Status	New

The size of the buffer used by EventThreadSpawn in InputEventWorker, at line 5342 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EventThreadSpawn passes to InputEventWorker, at line 5342 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5380	5380
Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void EventThreadSpawn(char *device)

```
....
5380.           memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=469
Status	New

The size of the buffer used by EventThreadSpawn in InputEventWorker, at line 5342 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EventThreadSpawn passes to InputEventWorker, at line 5342 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5380	5380
Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void EventThreadSpawn(char *device)

```
....
5380.           memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=470
Status	New

The size of the buffer used by ConfigureEvdevDevice in InputEventWorker, at line 5781 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ConfigureEvdevDevice passes to InputEventWorker, at line 5781 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5819	5819
Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
5819.           memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=471
Status	New

The size of the buffer used by ConfigureEvdevDevice in InputEventWorker, at line 5781 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ConfigureEvdevDevice passes to InputEventWorker, at line 5781 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	5819	5819
Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
5819.          memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=472
Status	New

The size of the buffer used by InitWindow in Namespace1167200667, at line 718 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitWindow passes to Namespace1167200667, at line 718 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	754	754
Object	Namespace1167200667	Namespace1167200667

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void InitWindow(int width, int height, const char *title)

```
....
754.      memset(&CORE.Input, 0, sizeof(CORE.Input));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=473
Status	New

The size of the buffer used by ConfigureEvdevDevice in InputEventWorker, at line 6048 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ConfigureEvdevDevice passes to InputEventWorker, at line 6048 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6086	6086

Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
6086.           memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=474
Status	New

The size of the buffer used by InitWindow in Namespace880858017, at line 718 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitWindow passes to Namespace880858017, at line 718 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	754	754
Object	Namespace880858017	Namespace880858017

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method void InitWindow(int width, int height, const char *title)

```
....
754.      memset(&CORE.Input, 0, sizeof(CORE.Input));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=475
Status	New

The size of the buffer used by ConfigureEvdevDevice in InputEventWorker, at line 6048 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ConfigureEvdevDevice passes to InputEventWorker, at line 6048 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-	raysan5@@raylib-4.2.0-CVE-2023-

	26123-FP.c	26123-FP.c
Line	6086	6086
Object	InputEventWorker	InputEventWorker

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
6086.          memset(worker, 0, sizeof(InputEventWorker));  // Clear
the worker
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=476
Status	New

The size of the buffer used by stb_vorbis_get_samples_float in k, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stb_vorbis_get_samples_float passes to k, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5465	5465
Object	k	k

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method int stb_vorbis_get_samples_float(stb_vorbis *f, int channels, float **buffer, int num_samples)

```
....
5465.              memcpy(buffer[i]+n, f->channel_buffers[i]+f-
>channel_buffer_start, sizeof(float)*k);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=477
Status	New

The size of the buffer used by stb_vorbis_get_samples_float in float, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that stb_vorbis_get_samples_float passes to float, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5465	5465
Object	float	float

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method int stb_vorbis_get_samples_float(stb_vorbis *f, int channels, float **buffer, int num_samples)

```
....
5465.              memcpy(buffer[i]+n, f->channel_buffers[i]+f-
>channel_buffer_start, sizeof(float)*k);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=478
Status New

The size of the buffer used by vorbis_decode_packet_rest in f, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that vorbis_decode_packet_rest passes to f, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3296	3296
Object	f	f

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3296.     memcpy(really_zero_channel, zero_channel,
sizeof(really_zero_channel[0]) * f->channels);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=479
Status	New

The size of the buffer used by vorbis_decode_packet_rest in really_zero_channel, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that vorbis_decode_packet_rest passes to really_zero_channel, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3296	3296
Object	really_zero_channel	really_zero_channel

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3296.     memcpy(really_zero_channel, zero_channel,
sizeof(really_zero_channel[0]) * f->channels);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=480
Status	New

The size of the buffer used by stb_vorbis_get_samples_float in k, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stb_vorbis_get_samples_float passes to k, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5467	5467
Object	k	k

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method int stb_vorbis_get_samples_float(stb_vorbis *f, int channels, float **buffer, int num_samples)

```
....
5467.             memset(buffer[i]+n, 0, sizeof(float) * k);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=481
Status	New

The size of the buffer used by stb_vorbis_get_samples_float in float, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that stb_vorbis_get_samples_float passes to float, at line 5453 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5467	5467
Object	float	float

Code Snippet

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method int stb_vorbis_get_samples_float(stb_vorbis *f, int channels, float **buffer, int num_samples)

```
....
5467.               memset(buffer[i]+n, 0, sizeof(float) * k);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=482
Status	New

The size of the buffer used by decode_residue in n, at line 2104 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_residue passes to n, at line 2104 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2127	2127
Object	n	n

Code Snippet

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2127.           memset(residue_buffers[i], 0, sizeof(float) * n);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=483
Status	New

The size of the buffer used by decode_residue in float, at line 2104 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that decode_residue passes to float, at line 2104 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2127	2127
Object	float	float

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2127.           memset(residue_buffers[i], 0, sizeof(float) * n);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=484
Status	New

The size of the buffer used by vorbis_decode_packet_rest in n2, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that vorbis_decode_packet_rest passes to n2, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3356	3356
Object	n2	n2

Code Snippet

File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3356.           memset(f->channel_buffers[i], 0, sizeof(*f-
>channel_buffers[i]) * n2);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=485
Status	New

The size of the buffer used by vorbis_decode_packet_rest in f, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that vorbis_decode_packet_rest passes to f, at line 3180 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3356	3356
Object	f	f

Code Snippet

File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int vorbis_decode_packet_rest(vorb *f, int *len, Mode *m, int left_start, int left_end, int right_start, int right_end, int *p_left)

```
....
3356.           memset(f->channel_buffers[i], 0, sizeof(*f-
>channel_buffers[i]) * n2);
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=515
Status	New

Calling free() (line 84) on a variable that was not dynamically allocated (line 84) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	87	87
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static ut8 *get_bytes(RBuffer *buffer, ut32 size) {

```
....
87.          free (ret);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=516
Status	New

Calling free() (line 270) on a variable that was not dynamically allocated (line 270) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	285	285
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_float_object(RBuffer *buffer) {

```
....
285.              free (ret);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=517
Status	New

Calling free() (line 323) on a variable that was not dynamically allocated (line 323) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	340	340
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
340.              free (ret);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=518
Status New

Calling free() (line 323) on a variable that was not dynamically allocated (line 323) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	345	345
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_complex_object(RBuffer *buffer) {

```
....
345.              free (ret);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=519
Status New

Calling free() (line 488) on a variable that was not dynamically allocated (line 488) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	495	495
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_array_object_generic(RBuffer *buffer, ut32 size) {

```
....
495.                free (ret);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=520
Status	New

Calling free() (line 488) on a variable that was not dynamically allocated (line 488) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	505	505
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_array_object_generic(RBuffer *buffer, ut32 size) {

```
....
505.                    free (ret);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=521
Status	New

Calling free() (line 825) on a variable that was not dynamically allocated (line 825) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	831	831
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_code_object(RBuffer *buffer) {

```
....
831.                free (ret);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=522
Status New

Calling free() (line 825) on a variable that was not dynamically allocated (line 825) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	832	832
Object	cobj	cobj

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_code_object(RBuffer *buffer) {

```
....
832.                free (cobj);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=523
Status New

Calling free() (line 825) on a variable that was not dynamically allocated (line 825) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	849	849
Object	ret	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_code_object(RBuffer *buffer) {

```
....
849.              free (ret);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=524
Status	New

Calling free() (line 825) on a variable that was not dynamically allocated (line 825) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	850	850
Object	cobj	cobj

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_code_object(RBuffer *buffer) {

```
....
850.              free (cobj);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=525
Status	New

Calling free() (line 825) on a variable that was not dynamically allocated (line 825) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	951	951
Object	cobj	cobj

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_code_object(RBuffer *buffer) {

```
....
951.                free (cobj);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=526
Status	New

Calling free() (line 1117) on a variable that was not dynamically allocated (line 1117) in file radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	1177	1177
Object	symbol	symbol

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static bool extract_sections_symbols(pyc_object *obj, RList *sections, RList *symbols, RList *cobjs, char *prefix) {

```
....
1177.       free (symbol);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=527
Status	New

Calling free() (line 398) on a variable that was not dynamically allocated (line 398) in file radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Line	412	412
Object	buf	buf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Method struct r_bin_te_obj_t* r_bin_te_new(const char* file) {

```
....
412.              free (buf);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=528
Status	New

Calling free() (line 398) on a variable that was not dynamically allocated (line 398) in file radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Line	415	415
Object	buf	buf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Method struct r_bin_te_obj_t* r_bin_te_new(const char* file) {

```
....
415.        free (buf);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=529
Status	New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	67	67
Object	ord	ord

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method static char *__func_name_from_ord(const char *module, ut16 ordinal) {

```
....
67.                free (ord);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=530
Status New

Calling free() (line 256) on a variable that was not dynamically allocated (line 256) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	259	259
Object	en	en

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method static void __free_resource_entry(void *entry) {

```
....
259.        free (en);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=531
Status New

Calling free() (line 262) on a variable that was not dynamically allocated (line 262) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	266	266
Object	res	res

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method static void __free_resource(void *resource) {

```
....
266.        free (res);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=532
Status New

Calling free() (line 353) on a variable that was not dynamically allocated (line 353) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	405	405
Object	entry	entry

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_entrypoints(r_bin_ne_obj_t *bin) {

```
....
405.                            free (entry);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=533
Status New

Calling free() (line 353) on a variable that was not dynamically allocated (line 353) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	412	412
Object	entry	entry

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_entrypoints(r_bin_ne_obj_t *bin) {

```
....
412.                                    free (entry);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=534
Status New

Calling free() (line 353) on a variable that was not dynamically allocated (line 353) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	421	421
Object	entry	entry

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_entrypoints(r_bin_ne_obj_t *bin) {

```
....
421.                                    free (entry);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=535
Status New

Calling free() (line 439) on a variable that was not dynamically allocated (line 439) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	533	533
Object	func	func

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
533.                                    free (func);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=536
Status New

Calling free() (line 439) on a variable that was not dynamically allocated (line 439) in file radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	535	535
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
535.                                free (name);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=537
Status New

Calling free() (line 51) on a variable that was not dynamically allocated (line 51) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	67	67
Object	ord	ord

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method static char *__func_name_from_ord(const char *module, ut16 ordinal) {

```
....
67.                free (ord);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=538
Status	New

Calling free() (line 256) on a variable that was not dynamically allocated (line 256) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	259	259
Object	en	en

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method static void __free_resource_entry(void *entry) {

```
....
259.        free (en);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=539
Status	New

Calling free() (line 262) on a variable that was not dynamically allocated (line 262) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	266	266
Object	res	res

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method static void __free_resource(void *resource) {

```
....
266.        free (res);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=540
Status New

Calling free() (line 353) on a variable that was not dynamically allocated (line 353) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	405	405
Object	entry	entry

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_entrypoints(r_bin_ne_obj_t *bin) {

```
....
405.                            free (entry);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=541
Status New

Calling free() (line 353) on a variable that was not dynamically allocated (line 353) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	412	412
Object	entry	entry

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_entrypoints(r_bin_ne_obj_t *bin) {

```
....
412.                                    free (entry);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=542
Status New

Calling free() (line 353) on a variable that was not dynamically allocated (line 353) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	421	421
Object	entry	entry

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_entrypoints(r_bin_ne_obj_t *bin) {

```
....
421.                                    free (entry);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=543
Status New

Calling free() (line 439) on a variable that was not dynamically allocated (line 439) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	533	533
Object	func	func

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
533.                                    free (func);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=544
Status New

Calling free() (line 439) on a variable that was not dynamically allocated (line 439) in file radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	535	535
Object	name	name

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
535.                                free (name);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=545
Status New

Calling free() (line 267) on a variable that was not dynamically allocated (line 267) in file radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	783	783
Object	flag_str	flag_str

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
783.        free (flag_str);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=546
Status	New

Calling free() (line 68) on a variable that was not dynamically allocated (line 68) in file radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Line	73	73
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Method static RList *entries(RBinFile *bf) {

```
....
73.         free (ptr);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=547
Status	New

Calling free() (line 68) on a variable that was not dynamically allocated (line 68) in file radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Line	78	78
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Method static RList *entries(RBinFile *bf) {

```
....
78.         free (ptr);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=548
Status New

Calling free() (line 245) on a variable that was not dynamically allocated (line 245) in file radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c	radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Line	308	308
Object	sym	sym

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-0302-FP.c
Method static RList *symbols(RBinFile *bf) {

```
....
308.                    free (sym);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=549
Status New

Calling free() (line 149) on a variable that was not dynamically allocated (line 149) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	155	155
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
155.              free (ptr);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=550
Status	New

Calling free() (line 149) on a variable that was not dynamically allocated (line 149) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	166	166
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
166.              free (ptr);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=551
Status	New

Calling free() (line 149) on a variable that was not dynamically allocated (line 149) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	171	171
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
171.              free (ptr);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=552
Status	New

Calling free() (line 186) on a variable that was not dynamically allocated (line 186) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	189	189
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_xcoff_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
189.              free (ptr);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=553
Status	New

Calling free() (line 186) on a variable that was not dynamically allocated (line 186) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	194	194
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_xcoff_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
194.              free (ptr);
```

MemoryFree on StackVariable\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=554
Status New

Calling free() (line 186) on a variable that was not dynamically allocated (line 186) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	201	201
Object	sn	sn

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_xcoff_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
201.        free (sn);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=555
Status New

Calling free() (line 186) on a variable that was not dynamically allocated (line 186) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	203	203
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinImport *_xcoff_fill_bin_import(struct r_bin_coff_obj *bin, int idx) {

```
....
203.              free (ptr);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=556
Status	New

Calling free() (line 345) on a variable that was not dynamically allocated (line 345) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	372	372
Object	tmp	tmp

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RList *sections(RBinFile *bf) {

```
....
372.                          free (tmp);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=557
Status	New

Calling free() (line 345) on a variable that was not dynamically allocated (line 345) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	376	376
Object	tmp	tmp

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RList *sections(RBinFile *bf) {

```
....
376.                    free (tmp);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=558
Status	New

Calling free() (line 389) on a variable that was not dynamically allocated (line 389) in file radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c may result with a crash.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	424	424
Object	ptr	ptr

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RList *symbols(RBinFile *bf) {

```
....
424.                        free (ptr);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=559
Status	New

Calling free() (line 61) on a variable that was not dynamically allocated (line 61) in file raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination

File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	98	98
Object	name	name

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method static _GLFWmonitor* createMonitor(DISPLAY_DEVICEW* adapter,

```
....
98.       free(name);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=560
Status New

Calling free() (line 62) on a variable that was not dynamically allocated (line 62) in file raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	99	99
Object	name	name

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method static _GLFWmonitor* createMonitor(DISPLAY_DEVICEW* adapter,

```
....
99.       free(name);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=561
Status New

Calling free() (line 62) on a variable that was not dynamically allocated (line 62) in file raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination

File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	99	99
Object	name	name

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method static _GLFWmonitor* createMonitor(DISPLAY_DEVICEW* adapter,

```
....
99.       free(name);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=562
Status New

Calling free() (line 3701) on a variable that was not dynamically allocated (line 3701) in file raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c may result with a crash.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	4264	4264
Object	configs	configs

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
4264.           free(configs);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=563
Status New

Calling free() (line 62) on a variable that was not dynamically allocated (line 62) in file raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c may result with a crash.

	Source	Destination

File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	99	99
Object	name	name

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method static _GLFWmonitor* createMonitor(DISPLAY_DEVICEW* adapter,

```
....
99.       free(name);
```

MemoryFree on StackVariable\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=564
Status New

Calling free() (line 3701) on a variable that was not dynamically allocated (line 3701) in file raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c may result with a crash.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	4264	4264
Object	configs	configs

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
4264.           free(configs);
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=423
Status New

The application performs an illegal operation in stb_vorbis_get_frame_short_interleaved, in raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c. In line 5296, the program attempts to divide by num_c, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input num_c in stb_vorbis_get_frame_short_interleaved of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, at line 5296.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5303	5303
Object	num_c	num_c

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method int stb_vorbis_get_frame_short_interleaved(stb_vorbis *f, int num_c, short *buffer, int num_shorts)

```
....
5303.        if (len*num_c > num_shorts) len = num_shorts / num_c;
```

Divide By Zero\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=424
Status New

The application performs an illegal operation in GetFPS, in raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c. In line 2099, the program attempts to divide by average, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input average in GetFPS of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, at line 2099.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2121	2121
Object	average	average

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method int GetFPS(void)

```
....
2121.       return (int)roundf(1.0f/average);
```

Divide By Zero\Path 3:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=425
Status	New

The application performs an illegal operation in GetFPS, in raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c. In line 2099, the program attempts to divide by average, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input average in GetFPS of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, at line 2099.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2121	2121
Object	average	average

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method int GetFPS(void)

```
....
2121.       return (int)roundf(1.0f/average);
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=426
Status	New

The application performs an illegal operation in GetFPS, in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c. In line 2593, the program attempts to divide by average, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input average in GetFPS of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, at line 2593.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2618	2618
Object	average	average

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method int GetFPS(void)

```
....
2618.       fps = (int)roundf(1.0f/average);
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=427
Status	New

The application performs an illegal operation in GetFPS, in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c. In line 2593, the program attempts to divide by average, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input average in GetFPS of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, at line 2593.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2618	2618
Object	average	average

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method int GetFPS(void)

```
....
2618.       fps = (int)roundf(1.0f/average);
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=428
Status	New

The application performs an illegal operation in GetFPS, in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c. In line 2698, the program attempts to divide by average, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input average in GetFPS of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, at line 2698.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2723	2723
Object	average	average

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method int GetFPS(void)

```
....
2723.       fps = (int)roundf(1.0f/average);
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=429
Status	New

The application performs an illegal operation in GetFPS, in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c. In line 2698, the program attempts to divide by average, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input average in GetFPS of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, at line 2698.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2723	2723
Object	average	average

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method int GetFPS(void)

```
....
2723.       fps = (int)roundf(1.0f/average);
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description

Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=941
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	514	587

Object	reloc	reloc

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
514.                                    free (reloc);
....
587.                               free (reloc);
```

Double Free\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=942
Status New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	514	587
Object	reloc	reloc

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method RList *r_bin_ne_get_relocs(r_bin_ne_obj_t *bin) {

```
....
514.                                    free (reloc);
....
587.                               free (reloc);
```

Double Free\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=943
Status New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	376	372
Object	tmp	tmp

Code Snippet

File Name	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method	static RList *sections(RBinFile *bf) {

```
....
376.                    free (tmp);
....
372.                         free (tmp);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=944
Status	New

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Line	538	671
Object	rel	rel

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method	static RList *_relocs_list(RBin *rbin, struct r_bin_coff_obj *bin, bool patch, ut64 imp_map) {

```
....
538.                    free (rel);
....
671.              free (rel);
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=623
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3888 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3890	3890
Object	AssignExpr	AssignExpr

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void ScrollCallback(GLFWwindow *window, double xoffset, double yoffset)

```
....
3890.       currentMouseWheelY = (int)yoffset;
```

Integer Overflow\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=624
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 523 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	559	559
Object	AssignExpr	AssignExpr

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static void xdgSurfaceHandleConfigure(void* userData,

```
....
559.                    height = width / targetRatio;
```

Integer Overflow\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=625
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 523 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	561	561
Object	AssignExpr	AssignExpr

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static void xdgSurfaceHandleConfigure(void* userData,

```
....
561.                    width = height * targetRatio;
```

Buffer Overflow AddressOfLocalVarReturned

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow AddressOfLocalVarReturned Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=434
Status	New

The pointer S_IFMT at raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c in line 3187 is being used after it has been freed.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	3192	3192
Object	S_IFMT	S_IFMT

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method bool IsPathFile(const char *path)

```
....
3192.       return S_ISREG(pathStat.st_mode);
```

Buffer Overflow AddressOfLocalVarReturned\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=435
Status	New

The pointer S_IFMT at raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c in line 3187 is being used after it has been freed.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	3192	3192
Object	S_IFMT	S_IFMT

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method bool IsPathFile(const char *path)

```
....
3192.       return S_ISREG(pathStat.st_mode);
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=621
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3894 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3950	3950
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static void KeyCallback(GLFWwindow *window, int key, int scancode, int action, int mods)

```
....
3950.       else currentKeyState[key] = action;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=622
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3954 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3957	3957
Object	AssignExpr	AssignExpr

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static void MouseButtonCallback(GLFWwindow *window, int button, int action, int mods)

```
....
3957.       currentMouseState[button] = action;
```

Stored Buffer Overflow boundcpy

Query Path:
CPP\Cx\CPP Stored Vulnerabilities\Stored Buffer Overflow boundcpy Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Stored Buffer Overflow boundcpy\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1278
Status	New

The size of the buffer used by getn in n, at line 1363 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get8 passes to fgetc, at line 1337 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	1367
Object	fgetc	n

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int getn(vorb *z, uint8 *data, int n)

```
....
1367.         memcpy(data, z->stream, n);
```

Stored Buffer Overflow boundcpy\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1279
Status	New

The size of the buffer used by getn in n, at line 1363 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that getn passes to data, at line 1363 of raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1373	1367
Object	data	n

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int getn(vorb *z, uint8 *data, int n)

```
....
1373.     if (fread(data, n, 1, z->f) == 1)
....
1367.        memcpy(data, z->stream, n);
```

Wrong Size t Allocation

Query Path:
CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=568
Status	New

The function size in radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c at line 169 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Line	210	210
Object	size	size

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0523-FP.c
Method static pyc_object *get_long_object(RBuffer *buffer) {

```
....
210.             hexstr = calloc (size, sizeof (char));
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Wrong Memory Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1277
Status	New

The function malloc in radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c at line 14 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c	radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Line	18	18
Object	sizeof	malloc

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-0695-FP.c
Method static int r_bin_te_init_hdr(struct r_bin_te_obj_t *bin) {

```
....
18.    if (!(bin->header = malloc (sizeof (TE_image_file_header)))) {
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description
Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=163
Status	New

The *r_debug_qnx_reg_profile method calls the strdup function, at line 262 of radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Line	267	267
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Method static char *r_debug_qnx_reg_profile(RDebug *dbg) {

```
....
267.                return strdup (
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=164
Status	New

The *r_debug_qnx_reg_profile method calls the strdup function, at line 262 of radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Line	296	296
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1207-FP.c
Method static char *r_debug_qnx_reg_profile(RDebug *dbg) {

```
....
296.                    return strdup (
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=165
Status	New

The *__resource_type_str method calls the strdup function, at line 181 of radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Line	253	253
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1237-FP.c
Method static char *__resource_type_str(int type) {

```
....
253.        return strdup (typeName);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=166
Status	New

The *__resource_type_str method calls the strdup function, at line 181 of radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c	radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Line	253	253
Object	strdup	strdup

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-1238-FP.c
Method static char *__resource_type_str(int type) {

```
....
253.        return strdup (typeName);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=167
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	344	344
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c

Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
344.                    snprintf (str, sizeof (str), " v%i, v%i", vA,
vB);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=168
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	350	350
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
350.                    snprintf (str, sizeof (str), " v%i, v%i", vA,
vB);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=169
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	356	356

Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
356.                    snprintf (str, sizeof (str), " v%i, v%i", vA,
vB);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=170
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	361	361
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
361.                    snprintf (str, sizeof (str), " v%i", vA);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=171
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	367	367
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
367.                    snprintf (str, sizeof (str), " v%i, %#x", vA,
vB);
```

Unchecked Return Value\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=172
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	374	374
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
374.                            snprintf (str, sizeof (str), " v%i,
%#04hx", vA, sB);
```

Unchecked Return Value\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=173
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	382	382
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
382.                          snprintf (str, sizeof (str), " v%i:v%i,
0x%08x", vA, vA + 1, vB);
```

Unchecked Return Value\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=174
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	384	384
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
384.                          snprintf (str, sizeof (str), " v%i,
0x%08x", vA, vB);
```

Unchecked Return Value\Path 13:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=175
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	393	393
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
393.                          snprintf (str, sizeof (str), " v%i:v%i,
0x%08x", vA, vA + 1, vB);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=176
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	395	395
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
395.                          snprintf (str, sizeof (str), " v%i,
0x%08x", vA, vB);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=177
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	412	412
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
412.                    snprintf (str, sizeof (str), " v%i, v%i, v%i",
vA, vB, vC);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=178
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	419	419
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
419.                    snprintf (str, sizeof (str), " v%i, v%i, %#x",
vA, vB, vC);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=179
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	426	426
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
426.                    snprintf (str, sizeof (str), " v%i, v%i, %#x",
vA, vB, vC);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=180
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	473	473
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
473.                            snprintf (str, sizeof (str), " {v%i}",
buf[4] & 0x0f);
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=181
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	476	476
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
476.                            snprintf (str, sizeof (str), " {v%i,
v%i}", buf[4] & 0x0f, (buf[4] & 0xf0) >> 4);
```

Unchecked Return Value\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=182
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	479	479
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
479.                          snprintf (str, sizeof (str), " {v%i, v%i, v%i}", buf[4] & 0x0f, (buf[4] & 0xf0) >> 4, buf[5] & 0x0f);
```

Unchecked Return Value\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=183
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	482	482
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
482.                          snprintf (str, sizeof (str), " {v%i, v%i, v%i, v%i}", buf[4] & 0x0f,
```

Unchecked Return Value\Path 22:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=184
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	486	486
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
486.                          snprintf (str, sizeof (str), " {}");
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=185
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	489	489
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
489.                    snprintf (str, sizeof (str), ", [%04x]", vB);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=186
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	497	497
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c

Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
497.                    snprintf (str, sizeof (str), " {v%i..v%i},
[%04x]", vC, vC + vA - 1, vB);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=187
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	505	505
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c

Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
505.                          snprintf (str, sizeof (str), " {v%i}",
buf[4] & 0x0f);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=188
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	508	508
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c

Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
508.                          snprintf (str, sizeof (str), " {v%i,
v%i}", buf[4] & 0x0f, (buf[4] & 0xf0) >> 4);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=189
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	511	511
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
511.                            snprintf (str, sizeof (str), " {v%i, v%i,
v%i}", buf[4] & 0x0f,
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=190
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	515	515
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
515.                            snprintf (str, sizeof (str), " {v%i, v%i,
v%i, v%i}", buf[4] & 0x0f,
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=191
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	519	519
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
519.                          snprintf (str, sizeof (str), " {}");
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=192
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	523	523
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
523.                      snprintf (str, sizeof (str), ", [%04x]", vB);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=193
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	532	532
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
532.                                    snprintf (str, sizeof (str), " v%i,
string+%i", vA, vB);
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=194
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	539	539
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
539.                                    snprintf (str, sizeof (str), " v%i,
class+%i", vA, vB);
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=195
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	541	541
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
541.                                snprintf (str, sizeof (str), " v%i, %s", vA, flag_str);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=196
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	546	546
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
546.                                    snprintf (str, sizeof (str), " v%i,
field+%i", vA, vB);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=197
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	548	548
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
548.                                    snprintf (str, sizeof (str), " v%i,
%s", vA, flag_str);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=198
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	559	559
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
559.                           snprintf (str, sizeof (str), " v%i, v%i,
[obj+%04x]", vA, vB, vC);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=199
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	570	570
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
570.                           snprintf (str, sizeof (str), " v%i,
thing+%i", vA, vB);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=200
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	583	583
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
583.                                    snprintf (str, sizeof (str), " v%i, v%i, %s", vA, vB, flag_str);
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=201
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	585	585
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
585.                                    snprintf (str, sizeof (str), " v%i, v%i, class+%i", vA, vB, vC);
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=202
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	590	590
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
590.                                    snprintf (str, sizeof (str), " v%i, v%i, %s", vA, vB, flag_str);
```

Unchecked Return Value\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=203
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	592	592
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
592.                                    snprintf (str, sizeof (str), " v%i, v%i, field+%i", vA, vB, vC);
```

Unchecked Return Value\Path 42:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=204
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	602	602
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
602.                          snprintf (str, sizeof (str), " v%i,
string+%i", vA, vB);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=205
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	615	615
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
615.                                snprintf (str, sizeof (str), "
{v%i..v%i}, %s", vC, vC + vA - 1, flag_str);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=206
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	618	618
Object	snprintf	snprintf

Code Snippet

File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c

Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
618.                                snprintf (str, sizeof (str), "
{v%i..v%i}, class+%i", vC, vC + vA - 1, vB);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=207
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	623	623
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
623.                                    snprintf (str, sizeof (str), "
{v%i..v%i}, %s", vC, vC + vA - 1, flag_str);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=208
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	626	626
Object	snprintf	snprintf

Code Snippet	
File Name	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method	static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
626.                                    snprintf (str, sizeof (str), "
{v%i..v%i}, call_site+%i", vC, vC + vA - 1, vB);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=209
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	631	631
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
631.                                    snprintf (str, sizeof (str), "
{v%i..v%i}, %s", vC, vC + vA - 1, flag_str);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=210
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	634	634
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
634.                                    snprintf (str, sizeof (str), "
{v%i..v%i}, method+%i", vC, vC + vA - 1, vB);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=211
Status	New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
644.                                    snprintf (str, sizeof (str), "
{v%i}", buf[4] & 0x0f);
```

Unchecked Return Value\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=212
Status New

The dalvik_disassemble method calls the snprintf function, at line 267 of radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c	radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Line	647	647
Object	snprintf	snprintf

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2022-28069-FP.c
Method static int dalvik_disassemble(RArchSession *as, RAnalOp *op, ut64 addr, const ut8 *buf, int len, int size) {

```
....
647.                                    snprintf (str, sizeof (str), " {v%i,
v%i}", buf[4] & 0x0f, (buf[4] & 0xf0) >> 4);
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1395
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	573	573
Object	VMIN	VMIN

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitTerminal(void)

```
....
573.        keyboardNewSettings.c_cc[VMIN] = 1;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1396
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	574	574
Object	VTIME	VTIME

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitTerminal(void)

```
....
574.        keyboardNewSettings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 3:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1397
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3668	3668
Object	GAMEPAD_BUTTON_LEFT_TRIGGER_2	GAMEPAD_BUTTON_LEFT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3668.                   currentGamepadState[msg->paramInt0][GAMEPAD_BUTTON_LEFT_TRIGGER_2] = (char)(gamepadAxisState[msg->paramInt0][GAMEPAD_AXIS_LEFT_TRIGGER] > 0.1);
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1398
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3669	3669
Object	GAMEPAD_BUTTON_RIGHT_TRIGGER_2	GAMEPAD_BUTTON_RIGHT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3669.                   currentGamepadState[msg->paramInt0][GAMEPAD_BUTTON_RIGHT_TRIGGER_2] = (char)(gamepadAxisState[msg->paramInt0][GAMEPAD_AXIS_RIGHT_TRIGGER] > 0.1);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1399
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3761	3761
Object	button	button

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3761.                       currentGamepadState[i][button] = 1;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1400
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3764	3764
Object	button	button

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3764.                   else currentGamepadState[i][button] = 0;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1401
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-	raysan5@@raylib-2.6.0-CVE-2023-

	26123-FP.c	26123-FP.c
Line	3773	3773
Object	axis	axis

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3773.                   gamepadAxisState[i][axis] = axes[k];
```

Unchecked Array Index\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1402
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3777	3777
Object	GAMEPAD_BUTTON_LEFT_TRIGGER_2	GAMEPAD_BUTTON_LEFT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3777.               currentGamepadState[i][GAMEPAD_BUTTON_LEFT_TRIGGER_2]
= (char)(gamepadAxisState[i][GAMEPAD_AXIS_LEFT_TRIGGER] > 0.1);
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1403
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3778	3778
Object	GAMEPAD_BUTTON_RIGHT_TRIGGER_2	GAMEPAD_BUTTON_RIGHT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3778.
currentGamepadState[i][GAMEPAD_BUTTON_RIGHT_TRIGGER_2] =
(char)(gamepadAxisState[i][GAMEPAD_AXIS_RIGHT_TRIGGER] > 0.1);
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1404
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3817	3817
Object	button	button

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3817.                       currentGamepadState[i][button] = 1;
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1405
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3820	3820
Object	button	button

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3820.                   else currentGamepadState[i][button] = 0;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1406
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3829	3829
Object	axis	axis

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
3829.                   gamepadAxisState[i][axis] = gamepadState.axis[j];
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1407
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3956	3956
Object	button	button

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void MouseButtonCallback(GLFWwindow *window, int button, int action, int mods)

```
....
3956.       previousMouseState[button] = currentMouseState[button];
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1408
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3957	3957
Object	button	button

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void MouseButtonCallback(GLFWwindow *window, int button, int action, int mods)

```
....
3957.       currentMouseState[button] = action;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1409
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4210	4210
Object	keycode	keycode

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static int32_t AndroidInputCallback(struct android_app *app, AInputEvent *event)

```
....
4210.               currentKeyState[keycode] = 1;  // Key down
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1410

Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4215	4215
Object	keycode	keycode

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static int32_t AndroidInputCallback(struct android_app *app, AInputEvent *event)

```
....
4215.           else currentKeyState[keycode] = 0;  // Key up
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1411
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4472	4472
Object	VMIN	VMIN

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitKeyboard(void)

```
....
4472.      keyboardNewSettings.c_cc[VMIN] = 1;
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1412
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c

Line	4473	4473
Object	VTIME	VTIME

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitKeyboard(void)

```
....
4473.       keyboardNewSettings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1413
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4991	4991
Object	MOUSE_MIDDLE_BUTTON	MOUSE_MIDDLE_BUTTON

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
4991.                   if (event.code == BTN_MIDDLE)
currentMouseStateEvdev[MOUSE_MIDDLE_BUTTON] =  event.value;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1414
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	619	619
Object	VMIN	VMIN

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c

Method	static void InitTerminal(void)

```
....
619.      keyboardNewSettings.c_cc[VMIN] = 1;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1415
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	620	620
Object	VTIME	VTIME

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method	static void InitTerminal(void)

```
....
620.      keyboardNewSettings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1416
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2117	2117
Object	index	index

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method	int GetFPS(void)

```
....
2117.          history[index] = fpsFrame/FPS_CAPTURE_FRAMES_COUNT;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1417
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4316	4316
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void PollInputEvents(void)

```
....
4316.                       CORE.Input.Gamepad.currentState[i][button] =
1;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1418
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4319	4319
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void PollInputEvents(void)

```
....
4319.                   else CORE.Input.Gamepad.currentState[i][button] =
0;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1419

Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4331	4331
Object	GAMEPAD_BUTTON_LEFT_TRIGGER_2	GAMEPAD_BUTTON_LEFT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void PollInputEvents(void)

```
....
4331.
CORE.Input.Gamepad.currentState[i][GAMEPAD_BUTTON_LEFT_TRIGGER_2] =
(char)(CORE.Input.Gamepad.axisState[i][GAMEPAD_AXIS_LEFT_TRIGGER] >
0.1);
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1420
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4332	4332
Object	GAMEPAD_BUTTON_RIGHT_TRIGGER_2	GAMEPAD_BUTTON_RIGHT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void PollInputEvents(void)

```
....
4332.
CORE.Input.Gamepad.currentState[i][GAMEPAD_BUTTON_RIGHT_TRIGGER_2] =
(char)(CORE.Input.Gamepad.axisState[i][GAMEPAD_AXIS_RIGHT_TRIGGER] >
0.1);
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1421
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4371	4371
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void PollInputEvents(void)

```
....
4371.                       CORE.Input.Gamepad.currentState[i][button] =
1;
```

Unchecked Array Index\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1422
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4374	4374
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void PollInputEvents(void)

```
....
4374.                   else CORE.Input.Gamepad.currentState[i][button] =
0;
```

Unchecked Array Index\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1423
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c

Line	4859	4859
Object	keycode	keycode

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static int32_t AndroidInputCallback(struct android_app *app, AInputEvent *event)

```
....
4859.                   CORE.Input.Keyboard.currentKeyState[keycode] = 1;
// Key down
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1424
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4864	4864
Object	keycode	keycode

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static int32_t AndroidInputCallback(struct android_app *app, AInputEvent *event)

```
....
4864.               else CORE.Input.Keyboard.currentKeyState[keycode] =
0;  // Key up
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1425
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5148	5148
Object	VMIN	VMIN

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method	static void InitKeyboard(void)

```
....
5148.       keyboardNewSettings.c_cc[VMIN] = 1;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1426
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5149	5149
Object	VTIME	VTIME

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method	static void InitKeyboard(void)

```
....
5149.       keyboardNewSettings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1427
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5664	5664
Object	MOUSE_MIDDLE_BUTTON	MOUSE_MIDDLE_BUTTON

Code Snippet	
File Name	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method	static void *EventThread(void *arg)

```
....
5664.                   if (event.code == BTN_MIDDLE)
CORE.Input.Mouse.currentButtonStateEvdev[MOUSE_MIDDLE_BUTTON] =
event.value;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1428
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	619	619
Object	VMIN	VMIN

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitTerminal(void)

```
....
619.      keyboardNewSettings.c_cc[VMIN] = 1;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1429
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	620	620
Object	VTIME	VTIME

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitTerminal(void)

```
....
620.      keyboardNewSettings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1430
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2117	2117
Object	index	index

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method int GetFPS(void)

```
....
2117.           history[index] = fpsFrame/FPS_CAPTURE_FRAMES_COUNT;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1431
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4316	4316
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
4316.                       CORE.Input.Gamepad.currentState[i][button] =
1;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1432

Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4319	4319
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
4319.                   else CORE.Input.Gamepad.currentState[i][button] =
0;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1433
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4331	4331
Object	GAMEPAD_BUTTON_LEFT_TRIGGER_2	GAMEPAD_BUTTON_LEFT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
4331.
CORE.Input.Gamepad.currentState[i][GAMEPAD_BUTTON_LEFT_TRIGGER_2] =
(char)(CORE.Input.Gamepad.axisState[i][GAMEPAD_AXIS_LEFT_TRIGGER] >
0.1);
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1434
Status	New

	Source	Destination

File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4332	4332
Object	GAMEPAD_BUTTON_RIGHT_TRIGGER_2	GAMEPAD_BUTTON_RIGHT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
4332.
CORE.Input.Gamepad.currentState[i][GAMEPAD_BUTTON_RIGHT_TRIGGER_2] =
(char)(CORE.Input.Gamepad.axisState[i][GAMEPAD_AXIS_RIGHT_TRIGGER] >
0.1);
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1435
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4371	4371
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
4371.                       CORE.Input.Gamepad.currentState[i][button] =
1;
```

Unchecked Array Index\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1436
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c

Line	4374	4374
Object	button	button

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void PollInputEvents(void)

```
....
4374.                   else CORE.Input.Gamepad.currentState[i][button] =
0;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1437
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4859	4859
Object	keycode	keycode

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static int32_t AndroidInputCallback(struct android_app *app, AInputEvent *event)

```
....
4859.                   CORE.Input.Keyboard.currentKeyState[keycode] = 1;
// Key down
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1438
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4864	4864
Object	keycode	keycode

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static int32_t AndroidInputCallback(struct android_app *app, AInputEvent *event)

```
....
4864.              else CORE.Input.Keyboard.currentKeyState[keycode] = 0;  // Key up
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1439
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5148	5148
Object	VMIN	VMIN

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitKeyboard(void)

```
....
5148.      keyboardNewSettings.c_cc[VMIN] = 1;
```

Unchecked Array Index\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1440
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5149	5149
Object	VTIME	VTIME

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitKeyboard(void)

```
....
5149.       keyboardNewSettings.c_cc[VTIME] = 0;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1441
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5664	5664
Object	MOUSE_MIDDLE_BUTTON	MOUSE_MIDDLE_BUTTON

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
5664.                   if (event.code == BTN_MIDDLE)
CORE.Input.Mouse.currentButtonStateEvdev[MOUSE_MIDDLE_BUTTON] =
event.value;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1442
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2614	2614
Object	index	index

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method int GetFPS(void)

```
....
2614.           history[index] = fpsFrame/FPS_CAPTURE_FRAMES_COUNT;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1443
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	4836	4836
Object	GAMEPAD_BUTTON_LEFT_TRIGGER_2	GAMEPAD_BUTTON_LEFT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void PollInputEvents(void)

```
....
4836.
CORE.Input.Gamepad.currentButtonState[i][GAMEPAD_BUTTON_LEFT_TRIGGER_2]
= (char)(CORE.Input.Gamepad.axisState[i][GAMEPAD_AXIS_LEFT_TRIGGER] >
0.1);
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1444
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	4837	4837
Object	GAMEPAD_BUTTON_RIGHT_TRIGGER_2	GAMEPAD_BUTTON_RIGHT_TRIGGER_2

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void PollInputEvents(void)

```
....
4837.
CORE.Input.Gamepad.currentButtonState[i][GAMEPAD_BUTTON_RIGHT_TRIGGER_2]
= (char)(CORE.Input.Gamepad.axisState[i][GAMEPAD_AXIS_RIGHT_TRIGGER] >
0.1);
```

Improper Resource Access Authorization

Query Path:

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1280
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6444	6444
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6444.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1281
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6457	6457
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6457.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1282
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6444	6444
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6444.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1283
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6457	6457
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6457.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1284

Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6712	6712
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6712.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1285
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6725	6725
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6725.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1286
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c

Line	6712	6712
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6712.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1287
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6725	6725
Object	fgets	fgets

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6725.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1288
Status New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1346	1346
Object	fgetc	fgetc

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c

Method	static uint8 get8(vorb *z)

```
....
1346.     int c = fgetc(z->f);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1289
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6444	6444
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6444.          fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1290
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6457	6457
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6457.              fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1291
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6444	6444
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6444.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1292
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6457	6457
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6457.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1293
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6712	6712
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6712.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1294
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6725	6725
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6725.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1295
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6712	6712

Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6712.           fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1296
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6725	6725
Object	buffer	buffer

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6725.               fgets(buffer, 256, repFile);
```

Improper Resource Access Authorization\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1297
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2204	2204
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method int StorageLoadValue(int position)

```
....
2204.              fread(&value, 4, 1, storageFile);   // Read 1 element
of 4 bytes size
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1298
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1373	1373
Object	data	data

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int getn(vorb *z, uint8 *data, int n)

```
....
1373.     if (fread(data, n, 1, z->f) == 1)
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1299
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5133	5133
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5133.              if (read(gamepadStream[i], &gamepadEvent,
sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1300
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4511	4511
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void ProcessKeyboard(void)

```
....
4511.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1301
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4896	4896
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
4896.          if (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=1302
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5187	5187
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void ProcessKeyboard(void)

```
....
5187.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1303
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5570	5570
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *EventThread(void *arg)

```
....
5570.          while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1304
Status	New

	Source	Destination

File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5797	5797
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1305
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5187	5187
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void ProcessKeyboard(void)

```
....
5187.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1306
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5570	5570

Object	Address	Address

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
5570.          while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1307
Status New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5797	5797
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
5797.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1308
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5640	5640
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c

Method	static void ProcessKeyboard(void)

```
....
5640.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1309
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6012	6012
Object	Address	Address

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static void PollKeyboardEvents(void)

```
....
6012.      while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1310
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6069	6069
Object	Address	Address

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static void *EventThread(void *arg)

```
....
6069.          while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1311
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6282	6282
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6282.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1312
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	5640	5640
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void ProcessKeyboard(void)

```
....
5640.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1313
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6012	6012
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void PollKeyboardEvents(void)

```
....
6012.       while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1314
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6069	6069
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void *EventThread(void *arg)

```
....
6069.           while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1315
Status	New

	Source	Destination

File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6282	6282
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void *GamepadThread(void *arg)

```
....
6282.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1316
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5906	5906
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ProcessKeyboard(void)

```
....
5906.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1317
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6280	6280

Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void PollKeyboardEvents(void)

```
....
6280.       while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
```

Improper Resource Access Authorization\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1318
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6337	6337
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void *EventThread(void *arg)

```
....
6337.           while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1319
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6550	6550
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.              if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1320
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	5906	5906
Object	keysBuffer	keysBuffer

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void ProcessKeyboard(void)

```
....
5906.      bufferByteCount = read(STDIN_FILENO, keysBuffer,
MAX_KEYBUFFER_SIZE);     // POSIX system call
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1321
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6280	6280
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void PollKeyboardEvents(void)

```
....
6280.      while (read(fd, &event, sizeof(event)) == (int)sizeof(event))
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1322
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6337	6337
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void *EventThread(void *arg)

```
....
6337.           while (read(worker->fd, &event, sizeof(event)) ==
(int)sizeof(event))
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1323
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6550	6550
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void *GamepadThread(void *arg)

```
....
6550.               if (read(CORE.Input.Gamepad.streamId[i],
&gamepadEvent, sizeof(struct js_event)) == (int)sizeof(struct js_event))
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=1324
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	922	922
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static void handleEvents(double* timeout)

```
....
922.                if (read(_glfw.wl.keyRepeatTimerfd, &repeats,
sizeof(repeats)) == 8)
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1325
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	942	942
Object	Address	Address

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static void handleEvents(double* timeout)

```
....
942.                if (read(_glfw.wl.cursorTimerfd, &repeats,
sizeof(repeats)) == 8)
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1326
Status	New

	Source	Destination

File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	991	991
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static char* readDataOfferAsString(struct wl_data_offer* offer, const char* mimeType)

```
....
991.          const ssize_t result = read(fds[0], string + length,
readSize);
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1327
Status New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	2301	2301
Object	buf	buf

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int ldbRepl(lua_State *lua) {

```
....
2301.              int nread = read(ldb.fd,buf,sizeof(buf));
```

Improper Resource Access Authorization\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1328
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6487	6487

Object	fprintf	fprintf

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6487.           fprintf(repFile, "# Automation events list\n");
```

Improper Resource Access Authorization\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1329
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6488	6488
Object	fprintf	fprintf

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6488.           fprintf(repFile, "#    c <events_count>\n");
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=584
Status New

The size of the buffer used by OpenURL in "explorer %s", at line 2218 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that OpenURL passes to "explorer %s", at line 2218 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2231	2231
Object	"explorer %s"	"explorer %s"

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method void OpenURL(const char *url)

```
....
2231.          sprintf(cmd, "explorer %s", url);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=585
Status	New

The size of the buffer used by InitEvdevInput in "%s%s", at line 4630 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 4630 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4657	4657
Object	"%s%s"	"%s%s"

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitEvdevInput(void)

```
....
4657.                  sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity-
>d_name);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=586
Status	New

The size of the buffer used by InitGamepad in "%s%i", at line 5083 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 5083 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5089	5089
Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitGamepad(void)

```
....
5089.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Potential Precision Problem\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=587
Status New

The size of the buffer used by OpenURL in "explorer %s", at line 2650 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "explorer %s", at line 2650 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2663	2663
Object	"explorer %s"	"explorer %s"

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
2663.           sprintf(cmd, "explorer %s", url);
```

Potential Precision Problem\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=588
Status New

The size of the buffer used by InitEvdevInput in "%s%s", at line 5302 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 5302 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5331	5331
Object	"%s%s"	"%s%s"

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void InitEvdevInput(void)

```
....
5331.                   sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity->d_name);
```

Potential Precision Problem\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=589
Status New

The size of the buffer used by InitGamepad in "%s%i", at line 5747 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 5747 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5753	5753
Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void InitGamepad(void)

```
....
5753.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Potential Precision Problem\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=590
Status	New

The size of the buffer used by OpenURL in "explorer %s", at line 2650 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "explorer %s", at line 2650 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2663	2663
Object	"explorer %s"	"explorer %s"

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method void OpenURL(const char *url)

```
....
2663.          sprintf(cmd, "explorer %s", url);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=591
Status	New

The size of the buffer used by InitEvdevInput in "%s%s", at line 5302 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 5302 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5331	5331
Object	"%s%s"	"%s%s"

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitEvdevInput(void)

```
....
5331.                  sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity-
>d_name);
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=592
Status	New

The size of the buffer used by InitGamepad in "%s%i", at line 5747 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 5747 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5753	5753
Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitGamepad(void)

```
....
5753.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=593
Status	New

The size of the buffer used by OpenURL in "explorer %s", at line 3245 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "explorer %s", at line 3245 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	3258	3258
Object	"explorer %s"	"explorer %s"

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
3258.           sprintf(cmd, "explorer %s", url);
```

Potential Precision Problem\Path 11:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=594
Status	New

The size of the buffer used by OpenURL in "xdg-open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "xdg-open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	3261	3261
Object	"xdg-open '%s'"	"xdg-open '%s'"

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
3261.           sprintf(cmd, "xdg-open '%s'", url); // Alternatives:
firefox, x-www-browser
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=595
Status	New

The size of the buffer used by OpenURL in "open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	3264	3264
Object	"open '%s'"	"open '%s'"

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
3264.           sprintf(cmd, "open '%s'", url);
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=596
Status	New

The size of the buffer used by EmscriptenGamepadCallback in "%s", at line 5549 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EmscriptenGamepadCallback passes to "%s", at line 5549 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5563	5563
Object	"%s"	"%s"

Code Snippet

File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c

Method static EM_BOOL EmscriptenGamepadCallback(int eventType, const EmscriptenGamepadEvent *gamepadEvent, void *userData)

```
....
5563.          sprintf(CORE.Input.Gamepad.name[gamepadEvent->index],"%s",gamepadEvent->id);
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=597
Status	New

The size of the buffer used by InitEvdevInput in "%s%s", at line 5742 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 5742 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5770	5770
Object	"%s%s"	"%s%s"

Code Snippet

File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c

Method static void InitEvdevInput(void)

```
....
5770.                   sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity-
>d_name);
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=598
Status	New

The size of the buffer used by InitGamepad in "%s%i", at line 6232 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 6232 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6238	6238
Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void InitGamepad(void)

```
....
6238.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=599
Status	New

The size of the buffer used by OpenURL in "explorer %s", at line 3245 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "explorer %s", at line 3245 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	3258	3258
Object	"explorer %s"	"explorer %s"

Code Snippet

File Name	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method	void OpenURL(const char *url)

```
....
3258.          sprintf(cmd, "explorer %s", url);
```

Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=600
Status	New

The size of the buffer used by OpenURL in "xdg-open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "xdg-open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	3261	3261
Object	"xdg-open '%s'"	"xdg-open '%s'"

Code Snippet

File Name	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method	void OpenURL(const char *url)

```
....
3261.          sprintf(cmd, "xdg-open '%s'", url); // Alternatives:
firefox, x-www-browser
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=601
Status	New

The size of the buffer used by OpenURL in "open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "open '%s'", at line 3245 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	3264	3264
Object	"open '%s'"	"open '%s'"

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method	void OpenURL(const char *url)

```
....
3264.           sprintf(cmd, "open '%s'", url);
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=602
Status	New

The size of the buffer used by EmscriptenGamepadCallback in "%s", at line 5549 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EmscriptenGamepadCallback passes to "%s", at line 5549 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	5563	5563
Object	"%s"	"%s"

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method	static EM_BOOL EmscriptenGamepadCallback(int eventType, const EmscriptenGamepadEvent *gamepadEvent, void *userData)

```
....
5563.           sprintf(CORE.Input.Gamepad.name[gamepadEvent-
>index],"%s",gamepadEvent->id);
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=603
Status	New

The size of the buffer used by InitEvdevInput in "%s%s", at line 5742 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 5742 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c

Line	5770	5770
Object	"%s%s"	"%s%s"

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void InitEvdevInput(void)

```
....
5770.                   sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity->d_name);
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=604
Status	New

The size of the buffer used by InitGamepad in "%s%i", at line 6232 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 6232 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6238	6238
Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void InitGamepad(void)

```
....
6238.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Potential Precision Problem\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=605
Status	New

The size of the buffer used by OpenURL in "explorer \"%s\"", at line 3385 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "explorer \"%s\"", at line 3385 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination

File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	3398	3398
Object	"explorer \"%s\""	"explorer \"%s\""

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
3398.           sprintf(cmd, "explorer \"%s\"", url);
```

Potential Precision Problem\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=606
Status	New

The size of the buffer used by OpenURL in "xdg-open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "xdg-open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	3401	3401
Object	"xdg-open '%s'"	"xdg-open '%s'"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
3401.           sprintf(cmd, "xdg-open '%s'", url); // Alternatives:
firefox, x-www-browser
```

Potential Precision Problem\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=607
Status	New

The size of the buffer used by OpenURL in "open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that OpenURL passes to "open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	3404	3404
Object	"open '%s'"	"open '%s'"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void OpenURL(const char *url)

```
....
3404.           sprintf(cmd, "open '%s'", url);
```

Potential Precision Problem\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=608
Status New

The size of the buffer used by ScanDirectoryFiles in "%s/%s", at line 5113 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ScanDirectoryFiles passes to "%s/%s", at line 5113 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5128	5128
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ScanDirectoryFiles(const char *basePath, FilePathList *files, const char *filter)

```
....
5128.                   sprintf(path, "%s/%s", basePath, dp->d_name);
```

Potential Precision Problem\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=609
Status New

The size of the buffer used by ScanDirectoryFilesRecursively in "%s/%s", at line 5152 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ScanDirectoryFilesRecursively passes to "%s/%s", at line 5152 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5167	5167
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ScanDirectoryFilesRecursively(const char *basePath, FilePathList *files, const char *filter)

```
....
5167.                   sprintf(path, "%s/%s", basePath, dp->d_name);
```

Potential Precision Problem\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=610
Status New

The size of the buffer used by EmscriptenGamepadCallback in "%s", at line 5762 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EmscriptenGamepadCallback passes to "%s", at line 5762 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5776	5776
Object	"%s"	"%s"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static EM_BOOL EmscriptenGamepadCallback(int eventType, const EmscriptenGamepadEvent *gamepadEvent, void *userData)

```
....
5776.          sprintf(CORE.Input.Gamepad.name[gamepadEvent-
>index],"%s",gamepadEvent->id);
```

Potential Precision Problem\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=611
Status	New

The size of the buffer used by InitEvdevInput in "%s%s", at line 6008 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 6008 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6037	6037
Object	"%s%s"	"%s%s"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void InitEvdevInput(void)

```
....
6037.                   sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity->d_name);
```

Potential Precision Problem\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=612
Status	New

The size of the buffer used by InitGamepad in "%s%i", at line 6500 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 6500 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6506	6506
Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void InitGamepad(void)

```
....
6506.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Potential Precision Problem\Path 30:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=613
Status	New

The size of the buffer used by OpenURL in "explorer \"%s\"", at line 3385 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "explorer \"%s\"", at line 3385 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	3398	3398
Object	"explorer \"%s\""	"explorer \"%s\""

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method void OpenURL(const char *url)

```
....
3398.           sprintf(cmd, "explorer \"%s\"", url);
```

Potential Precision Problem\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=614
Status	New

The size of the buffer used by OpenURL in "xdg-open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "xdg-open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	3401	3401
Object	"xdg-open '%s'"	"xdg-open '%s'"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method void OpenURL(const char *url)

```
....
3401.           sprintf(cmd, "xdg-open '%s'", url); // Alternatives:
firefox, x-www-browser
```

Potential Precision Problem\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=615
Status	New

The size of the buffer used by OpenURL in "open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that OpenURL passes to "open '%s'", at line 3385 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	3404	3404
Object	"open '%s'"	"open '%s'"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method void OpenURL(const char *url)

```
....
3404.          sprintf(cmd, "open '%s'", url);
```

Potential Precision Problem\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=616
Status	New

The size of the buffer used by ScanDirectoryFiles in "%s/%s", at line 5113 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ScanDirectoryFiles passes to "%s/%s", at line 5113 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	5128	5128
Object	"%s/%s"	"%s/%s"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void ScanDirectoryFiles(const char *basePath, FilePathList *files, const char *filter)

```
....
5128.                   sprintf(path, "%s/%s", basePath, dp->d_name);
```

Potential Precision Problem\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=617
Status	New

The size of the buffer used by ScanDirectoryFilesRecursively in "%s/%s", at line 5152 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ScanDirectoryFilesRecursively passes to "%s/%s", at line 5152 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	5167	5167
Object	"%s/%s"	"%s/%s"

Code Snippet

File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c

Method static void ScanDirectoryFilesRecursively(const char *basePath, FilePathList *files, const char *filter)

```
....
5167.                   sprintf(path, "%s/%s", basePath, dp->d_name);
```

Potential Precision Problem\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=618
Status	New

The size of the buffer used by EmscriptenGamepadCallback in "%s", at line 5762 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that EmscriptenGamepadCallback passes to "%s", at line 5762 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	5776	5776
Object	"%s"	"%s"

Code Snippet

File Name	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method	static EM_BOOL EmscriptenGamepadCallback(int eventType, const EmscriptenGamepadEvent *gamepadEvent, void *userData)

```
....
5776.          sprintf(CORE.Input.Gamepad.name[gamepadEvent->index],"%s",gamepadEvent->id);
```

Potential Precision Problem\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=619
Status	New

The size of the buffer used by InitEvdevInput in "%s%s", at line 6008 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitEvdevInput passes to "%s%s", at line 6008 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6037	6037
Object	"%s%s"	"%s%s"

Code Snippet

File Name	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method	static void InitEvdevInput(void)

```
....
6037.                  sprintf(path, "%s%s", DEFAULT_EVDEV_PATH, entity->d_name);
```

Potential Precision Problem\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=620
Status	New

The size of the buffer used by InitGamepad in "%s%i", at line 6500 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that InitGamepad passes to "%s%i", at line 6500 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c, to overwrite the target buffer.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6506	6506

Object	"%s%i"	"%s%i"

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void InitGamepad(void)

```
....
6506.           sprintf(gamepadDev, "%s%i", DEFAULT_GAMEPAD_DEV, i);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=389
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	147	147
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
147.            disconnected = calloc(_glfw.monitorCount,
sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=390
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Line	150	150
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2022-38890-FP.c
Method	void _glfwPollMonitorsWin32(void)

```
....
150.                 _glfw.monitorCount * sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=391
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2018	2018
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2018.       dirFilesPath = (char **)RL_MALLOC(sizeof(char
*)*MAX_DIRECTORY_FILES);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=392
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4071	4071
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method	static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
4071.      dropFilesPath = (char **)RL_MALLOC(sizeof(char *)*count);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=393
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2408	2408
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2408.      dirFilesPath = (char **)RL_MALLOC(sizeof(char
*)*MAX_DIRECTORY_FILES);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=394
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4717	4717
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
4717.      CORE.Window.dropFilesPath = (char **)RL_MALLOC(sizeof(char
*)*count);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=395
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	148	148
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
148.          disconnected = calloc(_glfw.monitorCount,
sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=396
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Line	151	151
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
151.                  _glfw.monitorCount * sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=397
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2408	2408
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2408.      dirFilesPath = (char **)RL_MALLOC(sizeof(char
*)*MAX_DIRECTORY_FILES);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=398
Status	New

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4717	4717
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
4717.      CORE.Window.dropFilesPath = (char **)RL_MALLOC(sizeof(char
*)*count);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=399
Status	New

	Source	Destination

File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	148	148
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
148.          disconnected = calloc(_glfw.monitorCount,
sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=400
Status New

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c	raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Line	151	151
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
151.                  _glfw.monitorCount * sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=401
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2906	2906
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2906.       dirFilesPath = (char
**)RL_MALLOC(MAX_DIRECTORY_FILES*sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=402
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5245	5245
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
5245.       CORE.Window.dropFilesPath = (char
**)RL_MALLOC(count*sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=403
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	148	148
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method	void _glfwPollMonitorsWin32(void)

```
....
148.          disconnected = calloc(_glfw.monitorCount,
sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=404
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Line	151	151
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
151.                  _glfw.monitorCount * sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=405
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2906	2906
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method char **GetDirectoryFiles(const char *dirPath, int *fileCount)

```
....
2906.      dirFilesPath = (char
**)RL_MALLOC(MAX_DIRECTORY_FILES*sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=406
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	5245	5245
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
5245.       CORE.Window.dropFilesPath = (char
**)RL_MALLOC(count*sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=407
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	3131	3131
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method FilePathList LoadDirectoryFiles(const char *dirPath)

```
....
3131.           files.paths = (char
**)RL_MALLOC(files.capacity*sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=408
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	3155	3155
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method FilePathList LoadDirectoryFilesEx(const char *basePath, const char *filter, bool scanSubdirs)

```
....
3155.       files.paths = (char **)RL_CALLOC(files.capacity, sizeof(char
*));
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=409
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5462	5462
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
5462.       CORE.Window.dropFilepaths = (char
**)RL_CALLOC(CORE.Window.dropFileCount, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=410
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	148	148
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
148.          disconnected = calloc(_glfw.monitorCount,
sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=411
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Line	151	151
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2022-38890-FP.c
Method void _glfwPollMonitorsWin32(void)

```
....
151.                  _glfw.monitorCount * sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=412
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c

Line	3131	3131
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method FilePathList LoadDirectoryFiles(const char *dirPath)

```
....
3131.          files.paths = (char
**)RL_MALLOC(files.capacity*sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=413
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	3155	3155
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method FilePathList LoadDirectoryFilesEx(const char *basePath, const char *filter, bool scanSubdirs)

```
....
3155.      files.paths = (char **)RL_CALLOC(files.capacity, sizeof(char
*));
```

Use of Sizeof On a Pointer Type\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=414
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	5462	5462
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method	static void WindowDropCallback(GLFWwindow *window, int count, const char **paths)

```
....
5462.       CORE.Window.dropFilepaths = (char
**)RL_CALLOC(CORE.Window.dropFileCount, sizeof(char *));
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=415
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3664	3664
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int start_decoder(vorb *f)

```
....
3664.         f->comment_list = (char**) setup_malloc(f, sizeof(char*) *
(f->comment_list_length));
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=416
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4173	4173
Object	sizeof	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int start_decoder(vorb *f)

```
....
4173.        classify_mem = f->channels * (sizeof(void*) + max_part_read
* sizeof(uint8 *));
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=417
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	4173	4173
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
4173.        classify_mem = f->channels * (sizeof(void*) + max_part_read
* sizeof(uint8 *));
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=418
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	374	374
Object	sizeof	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static void surfaceHandleEnter(void* userData,

```
....
374.                            window->wl.monitorsSize *
sizeof(_GLFWmonitor*));
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=419
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-21309-TP.c	redis@@redis-5.0.10-CVE-2021-21309-TP.c
Line	1045	1045
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-21309-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1045.               vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=420
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-21309-TP.c	redis@@redis-5.0.10-CVE-2021-21309-TP.c
Line	1051	1051
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-21309-TP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1051.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=421

Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	392	392
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisGenericCommand(lua_State *lua, int raise_error) {

```
....
392.          argv = zrealloc(argv,sizeof(robj*)*argc);
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=422
Status	New

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1463	1463
Object	sizeof	sizeof

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method void xreadCommand(client *c) {

```
....
1463.      if (groupname) groups =
zmalloc(sizeof(streamCG*)*streams_count);
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1362
Status	New

The StorageSaveValue method in raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2150	2150
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method void StorageSaveValue(int position, int value)

```
....
2150.       storageFile = fopen(path, "rb+");
```

TOCTOU\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1363
Status New

The StorageSaveValue method in raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2153	2153
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method void StorageSaveValue(int position, int value)

```
....
2153.       if (!storageFile) storageFile = fopen(path, "wb");
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1364
Status New

The StorageLoadValue method in raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2190	2190
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method int StorageLoadValue(int position)

```
....
2190.       FILE *storageFile = fopen(path, "rb");
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1365
Status New

The LoadAutomationEvents method in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6437	6437
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6437.       FILE *repFile = fopen(fileName, "rt");
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1366

Status	New

The ExportAutomationEvents method in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6483	6483
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6483.       FILE *repFile = fopen(fileName, "wt");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1367
Status	New

The LoadAutomationEvents method in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6437	6437
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6437.       FILE *repFile = fopen(fileName, "rt");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20

	053&pathid=1368
Status	New

The ExportAutomationEvents method in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6483	6483
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6483.       FILE *repFile = fopen(fileName, "wt");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1369
Status	New

The GetFileLength method in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2885	2885
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method int GetFileLength(const char *fileName)

```
....
2885.       FILE *file = fopen(fileName, "rb");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1370
Status	New

The LoadAutomationEvents method in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6705	6705
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6705.       FILE *repFile = fopen(fileName, "rt");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1371
Status	New

The ExportAutomationEvents method in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6751	6751
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6751.       FILE *repFile = fopen(fileName, "wt");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1372
Status	New

The GetFileLength method in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2885	2885
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method int GetFileLength(const char *fileName)

```
....
2885.       FILE *file = fopen(fileName, "rb");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1373
Status	New

The LoadAutomationEvents method in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6705	6705
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6705.       FILE *repFile = fopen(fileName, "rt");
```

TOCTOU\Path 13:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1374
Status	New

The ExportAutomationEvents method in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6751	6751
Object	fopen	fopen

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6751.       FILE *repFile = fopen(fileName, "wt");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1375
Status	New

The EventThreadSpawn method in raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	4715	4715
Object	open	open

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void EventThreadSpawn(char *device)

```
....
4715.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1376
Status	New

The InitGamepad method in raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	5091	5091
Object	open	open

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitGamepad(void)

```
....
5091.           if ((gamepadStream[i] = open(gamepadDev,
O_RDONLY|O_NONBLOCK)) < 0)
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1377
Status	New

The InitGraphicsDevice method in raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	3391	3391
Object	open	open

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
3391.       CORE.Window.fd = open(DEFAULT_GRAPHIC_DEVICE_DRM, O_RDWR);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1378
Status	New

The EventThreadSpawn method in raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5389	5389
Object	open	open

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void EventThreadSpawn(char *device)

```
....
5389.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1379
Status	New

The InitGamepad method in raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	5755	5755
Object	open	open

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void InitGamepad(void)

```
....
5755.          if ((CORE.Input.Gamepad.streamId[i] = open(gamepadDev,
O_RDONLY|O_NONBLOCK)) < 0)
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1380
Status	New

The InitGraphicsDevice method in raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	3391	3391
Object	open	open

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
3391.      CORE.Window.fd = open(DEFAULT_GRAPHIC_DEVICE_DRM, O_RDWR);
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1381
Status	New

The EventThreadSpawn method in raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5389	5389
Object	open	open

Code Snippet

File Name	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method	static void EventThreadSpawn(char *device)

```
....
5389.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1382
Status	New

The InitGamepad method in raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	5755	5755
Object	open	open

Code Snippet

File Name	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method	static void InitGamepad(void)

```
....
5755.           if ((CORE.Input.Gamepad.streamId[i] = open(gamepadDev,
O_RDONLY|O_NONBLOCK)) < 0)
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1383
Status	New

The InitGraphicsDevice method in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	4041	4041
Object	open	open

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static bool InitGraphicsDevice(int width, int height)

```
....
4041.       CORE.Window.fd = open(DEFAULT_GRAPHIC_DEVICE_DRM, O_RDWR);
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1384
Status	New

The ConfigureEvdevDevice method in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5828	5828
Object	open	open

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static void ConfigureEvdevDevice(char *device)

```
....
5828.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1385
Status	New

The InitGamepad method in raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6240	6240

Object	open	open

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void InitGamepad(void)

```
....
6240.          if ((CORE.Input.Gamepad.streamId[i] = open(gamepadDev,
O_RDONLY|O_NONBLOCK)) < 0)
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1386
Status	New

The InitGraphicsDevice method in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	4041	4041
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
4041.      CORE.Window.fd = open(DEFAULT_GRAPHIC_DEVICE_DRM, O_RDWR);
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1387
Status	New

The ConfigureEvdevDevice method in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c

Line	5828	5828
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
5828.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1388
Status	New

The InitGamepad method in raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6240	6240
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void InitGamepad(void)

```
....
6240.           if ((CORE.Input.Gamepad.streamId[i] = open(gamepadDev,
O_RDONLY|O_NONBLOCK)) < 0)
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1389
Status	New

The InitGraphicsDevice method in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	4218	4218
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
4218.       CORE.Window.fd = open(DEFAULT_GRAPHIC_DEVICE_DRM, O_RDWR);
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1390
Status	New

The ConfigureEvdevDevice method in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6095	6095
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
6095.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1391
Status	New

The InitGamepad method in raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6508	6508
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void InitGamepad(void)

```
....
6508.           if ((CORE.Input.Gamepad.streamId[i] = open(gamepadDev,
O_RDONLY | O_NONBLOCK)) < 0)
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1392
Status	New

The InitGraphicsDevice method in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	4218	4218
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static bool InitGraphicsDevice(int width, int height)

```
....
4218.       CORE.Window.fd = open(DEFAULT_GRAPHIC_DEVICE_DRM, O_RDWR);
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1393
Status	New

The ConfigureEvdevDevice method in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6095	6095
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void ConfigureEvdevDevice(char *device)

```
....
6095.       fd = open(device, O_RDONLY | O_NONBLOCK);
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1394
Status	New

The InitGamepad method in raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6508	6508
Object	open	open

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void InitGamepad(void)

```
....
6508.           if ((CORE.Input.Gamepad.streamId[i] = open(gamepadDev,
O_RDONLY | O_NONBLOCK)) < 0)
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection

NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=139
Status	New

Method GetRandomValue at line 1772 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	1781	1781
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method int GetRandomValue(int min, int max)

```
....
1781.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=140
Status	New

Method GetRandomValue at line 2200 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	2209	2209
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method int GetRandomValue(int min, int max)

```
....
2209.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=141
Status	New

Method GetRandomValue at line 2200 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	2209	2209
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method int GetRandomValue(int min, int max)

```
....
2209.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=142
Status	New

Method GetRandomValue at line 2683 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2692	2692
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method int GetRandomValue(int min, int max)

```
....
2692.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=143
Status	New

Method GetRandomValue at line 2683 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2692	2692
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method int GetRandomValue(int min, int max)

```
....
2692.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=144
Status	New

Method GetRandomValue at line 2793 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2802	2802
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method int GetRandomValue(int min, int max)

```
....
2802.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=145
Status	New

Method GetRandomValue at line 2793 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2802	2802
Object	rand	rand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method int GetRandomValue(int min, int max)

```
....
2802.       return (rand()%(abs(max - min) + 1) + min);
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=146
Status	New

Method luaRedisReplicateCommandsCommand at line 720 of redis@@redis-5.0.10-CVE-2021-32626-TP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32626-TP.c	redis@@redis-5.0.10-CVE-2021-32626-TP.c
Line	728	728
Object	rand	rand

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32626-TP.c
Method int luaRedisReplicateCommandsCommand(lua_State *lua) {

```
....
728.          redisSrand48(rand());
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=147
Status	New

Method InitTimer at line 3329 of raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	3331	3331
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method static void InitTimer(void)

```
....
3331.      srand((unsigned int)time(NULL));              // Initialize
random seed
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=148
Status	New

Method InitTimer at line 4081 of raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Line	4083	4083
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2021-3520-FP.c
Method static void InitTimer(void)

```
....
4083.      srand((unsigned int)time(NULL));                // Initialize
random seed
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=149
Status	New

Method InitTimer at line 4081 of raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c	raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Line	4083	4083
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-3.5.0-CVE-2023-26123-FP.c
Method static void InitTimer(void)

```
....
4083.      srand((unsigned int)time(NULL));                // Initialize
random seed
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=150
Status	New

Method InitWindow at line 697 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	789	789
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c

Method	void InitWindow(int width, int height, const char *title)

```
....
789.      srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=151
Status	New

Method SetRandomSeed at line 2696 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	2698	2698
Object	srand	srand

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	void SetRandomSeed(unsigned int seed)

```
....
2698.      srand(seed);
```

Use of Insufficiently Random Values\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=152
Status	New

Method AndroidCommandCallback at line 5259 of raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	5297	5297
Object	srand	srand

Code Snippet	
File Name	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method	static void AndroidCommandCallback(struct android_app *app, int32_t cmd)

```
....
5297.                    srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=153
Status	New

Method InitWindow at line 697 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	789	789
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method void InitWindow(int width, int height, const char *title)

```
....
789.      srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=154
Status	New

Method SetRandomSeed at line 2696 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	2698	2698
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method void SetRandomSeed(unsigned int seed)

```
....
2698.       srand(seed);
```

Use of Insufficiently Random Values\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=155
Status	New

Method AndroidCommandCallback at line 5259 of raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	5297	5297
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void AndroidCommandCallback(struct android_app *app, int32_t cmd)

```
....
5297.                       srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=156
Status	New

Method InitWindow at line 718 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	843	843
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void InitWindow(int width, int height, const char *title)

```
....
843.      srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=157
Status	New

Method SetRandomSeed at line 2806 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2808	2808
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method void SetRandomSeed(unsigned int seed)

```
....
2808.      srand(seed);
```

Use of Insufficiently Random Values\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=158
Status	New

Method AndroidCommandCallback at line 5474 of raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	5512	5512
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void AndroidCommandCallback(struct android_app *app, int32_t cmd)

```
....
5512.                    srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=159
Status	New

Method InitWindow at line 718 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	843	843
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method void InitWindow(int width, int height, const char *title)

```
....
843.      srand((unsigned int)time(NULL));
```

Use of Insufficiently Random Values\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=160
Status	New

Method SetRandomSeed at line 2806 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	2808	2808
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method void SetRandomSeed(unsigned int seed)

```
....
2808.       srand(seed);
```

Use of Insufficiently Random Values\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=161
Status	New

Method AndroidCommandCallback at line 5474 of raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	5512	5512
Object	srand	srand

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void AndroidCommandCallback(struct android_app *app, int32_t cmd)

```
....
5512.                       srand((unsigned int)time(NULL));
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=569
Status	New

The variable declared in null at radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c in line 752 is not initialized when it is used by ret at radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c in line 752.

	Source	Destination
File	radareorg@@radare2-5.9.0-CVE-2023-	radareorg@@radare2-5.9.0-CVE-2023-

	1605-FP.c	1605-FP.c
Line	756	756
Object	null	ret

Code Snippet
File Name radareorg@@radare2-5.9.0-CVE-2023-1605-FP.c
Method static RBinInfo *info(RBinFile *bf) {

```
....
756.        ret->file = bf->file? strdup (bf->file): NULL;
```

NULL Pointer Dereference\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=570
Status New

The variable declared in null at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346 is not initialized when it is used by data at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	373	435
Object	null	data

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method static BOOL CALLBACK deviceCallback(const DIDEVICEINSTANCE* di, void* user)

```
....
373.                                                NULL)))
....
435.      qsort(data.objects, data.objectCount,
```

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=571
Status New

The variable declared in null at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346 is not initialized when it is used by data at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346.

	Source	Destination

File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	373	435
Object	null	data

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method static BOOL CALLBACK deviceCallback(const DIDEVICEINSTANCE* di, void* user)

```
....
373.                                                NULL)))
....
435.      qsort(data.objects, data.objectCount,
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=572
Status	New

The variable declared in null at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346 is not initialized when it is used by data at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	373	448
Object	null	data

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method static BOOL CALLBACK deviceCallback(const DIDEVICEINSTANCE* di, void* user)

```
....
373.                                                NULL)))
....
448.          free(data.objects);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=573
Status	New

The variable declared in null at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346 is not initialized when it is used by data at raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c in line 346.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	373	476
Object	null	data

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method static BOOL CALLBACK deviceCallback(const DIDEVICEINSTANCE* di, void* user)

```
....
373.                                                NULL)))
....
476.          free(data.objects);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=574
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	2605	1033
Object	null	spi

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method void xinfoCommand(client *c) {

```
....
2605.                                          STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                  streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=575
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	2609	1033
Object	null	spi

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xinfoCommand(client *c) {

```
....
2609.                                                STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                    streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=576
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1057 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1073	1033

Object	null	spi

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method size_t streamReplyWithRangeFromConsumerPEL(client *c, stream *s, streamID *start, streamID *end, size_t count, streamConsumer *consumer) {

```
....
1073.                                       STREAM_RWR_RAWENTRIES,NULL) ==
0)
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=577
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1320 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1356	1033
Object	null	spi

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method void xrangeGenericCommand(client *c, int rev) {

```
....
1356.
streamReplyWithRange(c,s,&startid,&endid,count,rev,NULL,NULL,0,NULL);
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method	size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=578
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	2605	1033
Object	null	spi

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xinfoCommand(client *c) {

```
....
2605.                                       STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=579
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 2498 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	2609	1033
Object	null	spi

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method void xinfoCommand(client *c) {

```
....
2609.                                   STREAM_RWR_RAWENTRIES,NULL);
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=580
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1057 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1073	1033
Object	null	spi

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method size_t streamReplyWithRangeFromConsumerPEL(client *c, stream *s, streamID *start, streamID *end, size_t count, streamConsumer *consumer) {

```
....
1073.                                   STREAM_RWR_RAWENTRIES,NULL) ==
0)
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=581
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1320 is not initialized when it is used by spi at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 942.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1356	1033
Object	null	spi

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xrangeGenericCommand(client *c, int rev) {

```
....
1356.
streamReplyWithRange(c,s,&startid,&endid,count,rev,NULL,NULL,0,NULL);
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method size_t streamReplyWithRange(client *c, stream *s, streamID *start, streamID *end, size_t count, int rev, streamCG *group, streamConsumer *consumer, int flags, streamPropInfo *spi) {

```
....
1033.                   streamPropagateGroupID(c,spi->keyname,group,spi-
>groupname);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=582
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1211 is not initialized when it is used by s at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 398.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1286	402
Object	null	s

Code Snippet

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method void xaddCommand(client *c) {

```
....
1286.           &id, id_given ? &id : NULL)
```

File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c

Method int64_t streamTrimByLength(stream *s, size_t maxlen, int approx) {

```
....
402.      raxStart(&ri,s->rax);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=583
Status	New

The variable declared in null at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1770 is not initialized when it is used by s at redis@@redis-5.0.10-CVE-2021-32628-TP.c in line 1770.

	Source	Destination
File	redis@@redis-5.0.10-CVE-2021-32628-TP.c	redis@@redis-5.0.10-CVE-2021-32628-TP.c
Line	1780	1876
Object	null	s

Code Snippet
File Name redis@@redis-5.0.10-CVE-2021-32628-TP.c
Method void xgroupCommand(client *c) {

```
....
1780.       stream *s = NULL;
....
1876.                raxRemove(s->cgroups,(unsigned
char*)grpname,sdslen(grpname),NULL);
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1349
Status	New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2150	2150
Object	storageFile	storageFile

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method void StorageSaveValue(int position, int value)

```
....
2150.       storageFile = fopen(path, "rb+");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1350
Status	New

	Source	Destination

File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2153	2153
Object	storageFile	storageFile

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method void StorageSaveValue(int position, int value)

```
....
2153.       if (!storageFile) storageFile = fopen(path, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1351
Status New

	Source	Destination
File	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c	raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Line	2190	2190
Object	storageFile	storageFile

Code Snippet
File Name raysan5@@raylib-2.6.0-CVE-2023-26123-FP.c
Method int StorageLoadValue(int position)

```
....
2190.       FILE *storageFile = fopen(path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1352
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6437	6437
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6437.       FILE *repFile = fopen(fileName, "rt");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1353
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Line	6483	6483
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2021-3520-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6483.       FILE *repFile = fopen(fileName, "wt");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1354
Status New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6437	6437
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6437.       FILE *repFile = fopen(fileName, "rt");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1355
Status	New

	Source	Destination
File	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c	raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Line	6483	6483
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.0.0-CVE-2023-26123-TP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6483.       FILE *repFile = fopen(fileName, "wt");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1356
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	2885	2885
Object	file	file

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method int GetFileLength(const char *fileName)

```
....
2885.       FILE *file = fopen(fileName, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1357

Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6705	6705
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6705.       FILE *repFile = fopen(fileName, "rt");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1358
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Line	6751	6751
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2021-3520-FP.c
Method static void ExportAutomationEvents(const char *fileName)

```
....
6751.       FILE *repFile = fopen(fileName, "wt");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1359
Status	New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c

Line	2885	2885
Object	file	file

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method int GetFileLength(const char *fileName)

```
....
2885.       FILE *file = fopen(fileName, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1360
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6705	6705
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Method static void LoadAutomationEvents(const char *fileName)

```
....
6705.       FILE *repFile = fopen(fileName, "rt");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=1361
Status New

	Source	Destination
File	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c	raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c
Line	6751	6751
Object	repFile	repFile

Code Snippet
File Name raysan5@@raylib-4.2.0-CVE-2023-26123-FP.c

Method	static void ExportAutomationEvents(const char *fileName)

```
....
6751.      FILE *repFile = fopen(fileName, "wt");
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=626
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	1091	1091
Object	available	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static int compute_codewords(Codebook *c, uint8 *len, int n, uint32 *values)

```
....
1091.      memset(available, 0, sizeof(available));
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=627
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5185	5185
Object	buffer	sizeof

Code Snippet	
File Name	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method	static void compute_samples(int mask, short *output, int num_c, float **data, int d_offset, int len)

```
....
5185.        memset(buffer, 0, sizeof(buffer));
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=628
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	5214	5214
Object	buffer	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void compute_stereo_samples(short *output, int num_c, float **data, int d_offset, int len)

```
....
5214.        memset(buffer, 0, sizeof(buffer));
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=629
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2118	2118
Object	Pointer	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2118.     uint8 ***part_classdata = (uint8 ***) temp_block_array(f,f->channels, part_read * sizeof(**part_classdata));
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=630
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2118	2118
Object	Pointer	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2118.     uint8 ***part_classdata = (uint8 ***) temp_block_array(f,f->channels, part_read * sizeof(**part_classdata));
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=631
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2118	2118
Object	Pointer	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2118.     uint8 ***part_classdata = (uint8 ***) temp_block_array(f,f->channels, part_read * sizeof(**part_classdata));
```

Sizeof Pointer Argument\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=632
Status	New

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	2118	2118
Object	Pointer	sizeof

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static void decode_residue(vorb *f, float *residue_buffers[], int ch, int n, int rn, uint8 *do_not_decode)

```
....
2118.     uint8 ***part_classdata = (uint8 ***) temp_block_array(f,f->channels, part_read * sizeof(**part_classdata));
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description
Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=430
Status	New

The buffer allocated by <= in raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c at line 346 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	357	357
Object	<=	<=

Code Snippet
File Name raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c

Method	static BOOL CALLBACK deviceCallback(const DIDEVICEINSTANCE* di, void* user)

```
....
357.      for (jid = 0;  jid <= GLFW_JOYSTICK_LAST;  jid++)
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=431
Status	New

The buffer allocated by <= in raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c at line 496 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	509	509
Object	<=	<=

Code Snippet	
File Name	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method	void _glfwDetectJoystickConnectionWin32(void)

```
....
509.              for (jid = 0;  jid <= GLFW_JOYSTICK_LAST;  jid++)
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=432
Status	New

The buffer allocated by <= in raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c at line 556 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Line	560	560
Object	<=	<=

Code Snippet	
File Name	raysan5@@raylib-3.7.0-CVE-2021-3520-FP.c
Method	void _glfwDetectJoystickDisconnectionWin32(void)

```
....
560.      for (jid = 0;  jid <= GLFW_JOYSTICK_LAST;  jid++)
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=433
Status	New

The buffer allocated by <= in raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c at line 3580 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c	raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Line	3963	3963
Object	<=	<=

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2021-3520-FP.c
Method static int start_decoder(vorb *f)

```
....
3963.           for (j=0; j <= max_class; ++j) {
```

Potential Path Traversal

Query Path:
CPP\Cx\CPP Low Visibility\Potential Path Traversal Version:0

Categories

OWASP Top 10 2013: A4-Insecure Direct Object References
OWASP Top 10 2017: A5-Broken Access Control

Description

Potential Path Traversal\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020064&projectid=20053&pathid=162
Status	New

Method createAnonymousFile at line 86 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c gets user input from the getenv element. This element's value then flows through the code and is eventually used in a file path for local disk access in createTmpfileCloexec at line 55 of raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c. This may cause a Path Traversal vulnerability.

	Source	Destination

File	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c	raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Line	111	61
Object	getenv	tmpname

Code Snippet
File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static int createAnonymousFile(off_t size)

```
....
111.          path = getenv("XDG_RUNTIME_DIR");
```

File Name raysan5@@raylib-4.5.0-CVE-2022-38890-FP.c
Method static int createTmpfileCloexec(char* tmpname)

```
....
61.          unlink(tmpname);
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow unbounded

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow OutOfBound

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

Dangerous Functions

Risk

What might happen

Use of dangerous functions may expose varying risks associated with each particular function, with potential impact of improper usage of these functions varying significantly. The presence of such functions indicates a flaw in code maintenance policies and adherence to secure coding practices, in a way that has allowed introducing known dangerous code into the application.

Cause

How does it happen

A dangerous function has been identified within the code. Functions are often deemed dangerous to use for numerous reasons, as there are different sets of vulnerabilities associated with usage of such functions. For example, some string copy and concatenation functions are vulnerable to Buffer Overflow, Memory Disclosure, Denial of Service and more. Use of these functions is not recommended.

General Recommendations

How to avoid it

- Deploy a secure and recommended alternative to any functions that were identified as dangerous.
    - If no secure alternative is found, conduct further researching and testing to identify whether current usage successfully sanitizes and verifies values, and thus successfully avoids the use-cases for whom the function is indeed dangerous
- Conduct a periodical review of methods that are in use, to ensure that all external libraries and built-in functions are up-to-date and whose use has not been excluded from best secure coding practices.

Source Code Examples

CPP

Buffer Overflow in gets()

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	gets(buf); // veryveryverylongname
	if (buf == ACCEPTED_NAME)
	{
		// Do something
	}
	return 0;
}
```

Safe reading from user

```
int main()
{
	char buf[10];

	printf("Please enter your name: ");
	fgets(buf, sizeof(buf), stdin); //setting the amount of bytes to read
	if (buf == ACCEPTED_NAME)
	{
		//Do something
	}
	return 0;
}
```

Unsafe function for string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strcpy(buf, argv[1]); // overflow occurs when len(argv[1]) > 10 bytes

	return 0;
}
```

Safe string copy

```
int main(int argc, char* argv[])
{
	char buf[10];
	strncpy(buf, argv[1], sizeof(buf));
	buf[9]= '\0'; //strncpy doesn't NULL terminates

	return 0;
}
```

Unsafe format string

```
int main(int argc, char* argv[])
{
	printf(argv[1]); // If argv[1] contains a format token, such as %s,%x or %d, will cause
an access violation
	return 0;
}
```

Safe format string

```
int main(int argc, char* argv[])
{
      printf("%s", argv[1]); // Second parameter is not a formattable string
      return 0;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities have two common (and sometimes overlapping) causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Wrong Memory Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
```

```
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Stored Buffer Overflow boundcpy

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Potential Path Traversal

Risk

What might happen

An attacker could define any arbitrary file path for the application to use, potentially leading to:

- Stealing sensitive files, such as configuration or system files
- Overwriting files such as program binaries, configuration files, or system files
- Deleting critical files, causing a denial of service (DoS).

Cause

How does it happen

The application uses user input in the file path for accessing files on the application server's local disk. This enables an attacker to arbitrarily determine the file path.

General Recommendations

How to avoid it

1. Ideally, avoid depending on user input for file selection.
2. Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified structure, rather than reject bad patterns. Check for:
   - Data type
   - Size
   - Range
   - Format
   - Expected values
3. Accept user input only for the filename, not for the path and folders.
4. Ensure that file path is fully canonicalized.
5. Explicitly limit the application to using a designated folder that separate from the applications binary folder.
6. Restrict the privileges of the application's OS user to necessary files and folders. The application should not be able to write to the application binary folder, and should not read anything outside of the application folder and data folder.

Source Code Examples

CSharp

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class PathTraversal
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text;
                string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
```

```
        }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class PathTraversalFixed
{
        private void foo(TextBox textbox1)
    {
                string fileNum = textbox1.Text.Replace("\", "").Replace("..", "");
         string path = "c:\files\file" + fileNum;
                FileStream f = new FileStream(path, FileMode.Open);
                byte[] output = new byte[10];
                f.Read(output,0, 10);
        }
}
```

Java

Using unvalidated user input as the file name may enable the user to access arbitrary files on the server local disk

```
public class Absolute_Path_Traversal {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Potentially hazardous characters are removed from the user input before use

```
public class Absolute_Path_Traversal_Fixed {
    public static void main(String[] args) {
        Scanner userInputScanner = new Scanner(System.in);
        System.out.print("\nEnter file name: ");
        String name = userInputScanner.nextLine();
        name = name.replace("/", "").replace("..", "");
        String path = "c:\files\file" + name;
        try {
            BufferedReader reader = new BufferedReader(new FileReader(path));
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

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.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

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.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that

identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Insecure Permission Assignment for Resource		
2009-05-27	Insecure Permission Assignment for Critical Resource		

BACK TO TOP

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
	public static int counter = 0;
	public static void start() throws InterruptedException {
		incrementCounter ic;
		decrementCounter dc;
		while(counter == 0) {
			counter = 0;
			ic = new incrementCounter();
			dc = new decrementCounter();
			ic.start();
			dc.start();
			ic.join();
			dc.join();
		}
		System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
	}

	public static class incrementCounter extends Thread {
	    public void run() {
		counter++;
	    }
```

```
    }

    public static class decrementCounter extends Thread {
        public void run() {
           counter--;
        }
    }
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
    public static int counter = 0;
    public static Object lock = new Object();

    public static void start() throws InterruptedException {
           incrementCounter ic;
           decrementCounter dc;
           while(counter == 0) { // because of proper locking, this condition is never false
                  counter = 0;
                  ic = new incrementCounter();
                  dc = new decrementCounter();
                  ic.start();
                  dc.start();
                  ic.join();
                  dc.join();
           }
           System.out.println(counter); // Never reached
    }

    public static class incrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter++;
           }
        }
    }

    public static class decrementCounter extends Thread {
        public void run() {
           synchronized (lock) {
                  counter--;
           }
        }
    }
```

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

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.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
```

```
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);
```

```
} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025