vul_files_31 Scan Report

Project Name	vul_files_31
Scan Start	Tuesday, January 7, 2025 3:41:58 PM
Preset	Checkmarx Default
Scan Time	03h:10m:46s
Lines Of Code Scanned	289502
Files Scanned	124
Report Creation Time	Tuesday, January 7, 2025 7:02:40 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	9/10000 (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

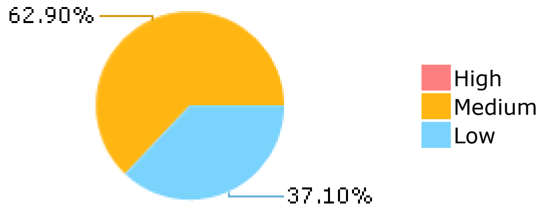
Results Limit

Results limit per query was set to 50

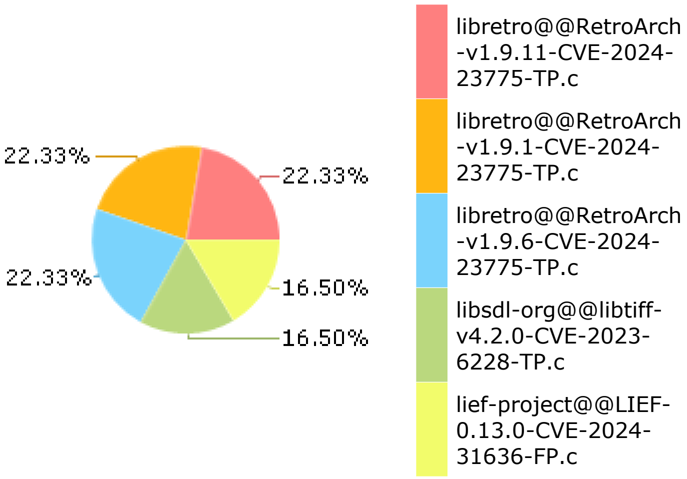
Selected Queries

Selected queries are listed in Result Summary

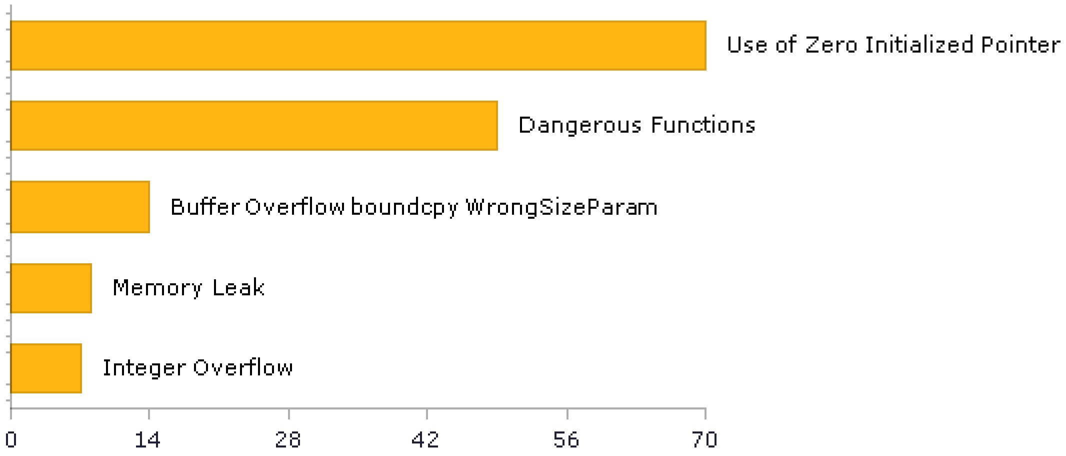
Result Summary



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	25	23
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	47	47
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	7	7
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	0	0
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	49	49
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	0	0
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	49	49
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	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	24	24
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.	1	1
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.	46	46
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.	7	7
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.	10	10

* 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)	47	47
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)	7	7
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*****	89	62
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	14	14
SI-11 Error Handling (P2)*****	12	12
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	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 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

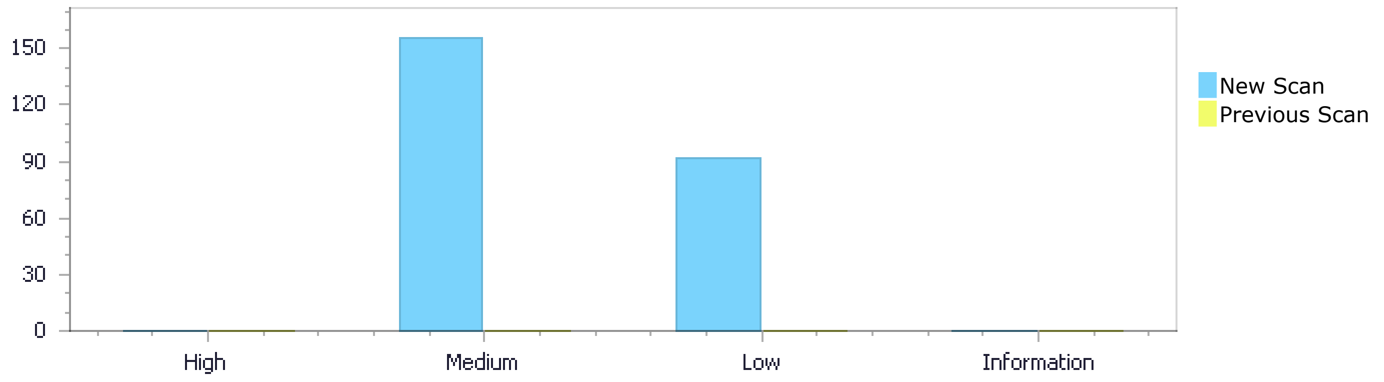
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	0	156	92	0	248
Recurrent Issues	0	0	0	0	0
Total	0	156	92	0	248

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	0	156	92	0	248
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	0	156	92	0	248

Result Summary

Vulnerability Type	Occurrences	Severity
Use of Zero Initialized Pointer	70	Medium
Dangerous Functions	49	Medium
Buffer Overflow boundcpy WrongSizeParam	14	Medium
Memory Leak	8	Medium
Integer Overflow	7	Medium

Divide By Zero	5	Medium
Float Overflow	3	Medium
Improper Resource Access Authorization	46	Low
Unchecked Return Value	12	Low
NULL Pointer Dereference	11	Low
Use of Sizeof On a Pointer Type	8	Low
Use of Insufficiently Random Values	7	Low
Unchecked Array Index	4	Low
Inconsistent Implementations	2	Low
Incorrect Permission Assignment For Critical Resources	1	Low
TOCTOU	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	20
libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	20
libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	20
libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	9
libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	9
libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	7
libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c	3
libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c	3
libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	3
libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c	3

Scan Results Details

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=1020040&projectid=20033&pathid=89
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	829	847
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
829.                    video_decoder_context_t *ctx = NULL;
....
847.                    stride                       = ctx->target-
>linesize[0];
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=90
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607.

	Source	Destination

File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	829	846
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
829.                video_decoder_context_t *ctx = NULL;
....
846.                src                           = ctx->target-
>data[0];
```

Use of Zero Initialized Pointer\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=91
Status New

The variable declared in ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	829	833
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
829.                video_decoder_context_t *ctx = NULL;
....
833.                pts                           = ctx->pts;
```

Use of Zero Initialized Pointer\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=92
Status New

The variable declared in ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	928	933
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.              video_decoder_context_t *ctx = NULL;
....
933.              stride                   = ctx->target-
>linesize[0];
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=93
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	928	932
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.              video_decoder_context_t *ctx = NULL;
....
932.              src                      = ctx->target-
>data[0];
```

Use of Zero Initialized Pointer\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=94
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	928	931
Object	ctx	ctx

Code Snippet

File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c

Method void CORE_PREFIX(retro_run)(void)

```
....
928.                 video_decoder_context_t *ctx = NULL;
....
931.                 pts                          = ctx->pts;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=95
Status	New

The variable declared in decoder_ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 1509 is not initialized when it is used by decoder_ctx at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 1509.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	1515	1544
Object	decoder_ctx	decoder_ctx

Code Snippet

File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c

Method static void decode_video(AVCodecContext *ctx, AVPacket *pkt, size_t frame_size, ASS_Track *ass_track_active)

```
....
1515.     video_decoder_context_t *decoder_ctx = NULL;
....
1544.        ret = avcodec_receive_frame(ctx, decoder_ctx->source);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=96
Status	New

The variable declared in audio_buffer at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 1709 is not initialized when it is used by audio_buffer at libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c in line 1709.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	1716	1832
Object	audio_buffer	audio_buffer

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method static void decode_thread(void *data)

```
....
1716.      int16_t *audio_buffer    = NULL;
....
1832.            audio_buffer = decode_audio(actx_active, pkt, aud_frame,
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=97
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	829	847
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
829.                 video_decoder_context_t *ctx = NULL;
....
847.                 stride                       = ctx->target-
>linesize[0];
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=98
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	829	846
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
829.                 video_decoder_context_t *ctx = NULL;
....
846.                 src                          = ctx->target-
>data[0];
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=99
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	829	833
Object	ctx	ctx

Code Snippet	
File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
829.                    video_decoder_context_t *ctx = NULL;
....
833.                    pts                         = ctx->pts;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=100
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	928	933
Object	ctx	ctx

Code Snippet	
File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
928.                    video_decoder_context_t *ctx = NULL;
....
933.                    stride                      = ctx->target-
>linesize[0];
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=101
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c

Line	928	932
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.                    video_decoder_context_t *ctx = NULL;
....
932.                    src                           = ctx->target-
>data[0];
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=102
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	928	931
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.                    video_decoder_context_t *ctx = NULL;
....
931.                    pts                           = ctx->pts;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=103
Status	New

The variable declared in decoder_ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 1509 is not initialized when it is used by decoder_ctx at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 1509.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	1515	1544
Object	decoder_ctx	decoder_ctx

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	static void decode_video(AVCodecContext *ctx, AVPacket *pkt, size_t frame_size, ASS_Track *ass_track_active)

```
....
1515.     video_decoder_context_t *decoder_ctx = NULL;
....
1544.        ret = avcodec_receive_frame(ctx, decoder_ctx->source);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=104
Status	New

The variable declared in audio_buffer at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 1709 is not initialized when it is used by audio_buffer at libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c in line 1709.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	1716	1832
Object	audio_buffer	audio_buffer

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	static void decode_thread(void *data)

```
....
1716.     int16_t *audio_buffer    = NULL;
....
1832.           audio_buffer = decode_audio(actx_active, pkt, aud_frame,
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=105
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	829	847
Object	ctx	ctx

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
829.                video_decoder_context_t *ctx = NULL;
....
847.                stride                      = ctx->target-
>linesize[0];
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=106
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	829	846
Object	ctx	ctx

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
829.                video_decoder_context_t *ctx = NULL;
....
846.                src                         = ctx->target-
>data[0];
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=107
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	829	833
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
829.                    video_decoder_context_t *ctx = NULL;
....
833.                    pts                           = ctx->pts;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=108
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	928	933
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.                    video_decoder_context_t *ctx = NULL;
....
933.                    stride                        = ctx->target-
>linesize[0];
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=109
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	928	932
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.                    video_decoder_context_t *ctx = NULL;
....
932.                    src                          = ctx->target-
>data[0];
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=110
Status	New

The variable declared in ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607 is not initialized when it is used by ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 607.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	928	931
Object	ctx	ctx

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
928.                    video_decoder_context_t *ctx = NULL;
....
931.                    pts                            = ctx->pts;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=111
Status	New

The variable declared in decoder_ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 1509 is not initialized when it is used by decoder_ctx at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 1509.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	1515	1544
Object	decoder_ctx	decoder_ctx

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method	static void decode_video(AVCodecContext *ctx, AVPacket *pkt, size_t frame_size, ASS_Track *ass_track_active)

```
....
1515.     video_decoder_context_t *decoder_ctx = NULL;
....
1544.        ret = avcodec_receive_frame(ctx, decoder_ctx->source);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=112
Status	New

The variable declared in audio_buffer at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 1709 is not initialized when it is used by audio_buffer at libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c in line 1709.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	1716	1832

Object	audio_buffer	audio_buffer

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method static void decode_thread(void *data)

```
....
1716.     int16_t *audio_buffer    = NULL;
....
1832.           audio_buffer = decode_audio(actx_active, pkt, aud_frame,
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=113
Status	New

The variable declared in texturedata at libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c in line 605 is not initialized when it is used by texturedata at libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c in line 605.

	Source	Destination
File	libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c	libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c
Line	610	656
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
610.      GLES_TextureData *texturedata = NULL;
....
656.                *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=114
Status	New

The variable declared in texturedata at libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c in line 605 is not initialized when it is used by texturedata at libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c in line 605.

	Source	Destination

File	libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c	libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c
Line	610	655
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
610.      GLES_TextureData *texturedata = NULL;
....
655.              *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=115
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c in line 595 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c in line 595.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c
Line	600	646
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
600.      GLES_TextureData *texturedata = NULL;
....
646.              *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=116
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c in line 595 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c in line 595.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c
Line	600	645
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
600.      GLES_TextureData *texturedata = NULL;
....
645.              *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=117
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c in line 602 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c in line 602.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c	libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c
Line	607	653
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
607.      GLES_TextureData *texturedata = NULL;
....
653.              *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=118
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c in line 602 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c in line 602.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c	libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c
Line	607	652
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-prerelease-2.25.1-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
607.      GLES_TextureData *texturedata = NULL;
....
652.              *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=119
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c	libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c
Line	598	644
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c
Method static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.        GLES_TextureData *texturedata = NULL;
....
644.                *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=120
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c	libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c
Line	598	643
Object	texturedata	texturedata

Code Snippet

File Name	libsdl-org@@SDL-prerelease-2.27.1-CVE-2022-4743-FP.c
Method	static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.        GLES_TextureData *texturedata = NULL;
....
643.                *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=121
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c	libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c
Line	598	644

Object	texturedata	texturedata

Code Snippet

File Name	libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c
Method	static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.      GLES_TextureData *texturedata = NULL;
....
644.              *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=122
Status	New

The variable declared in texturedata at libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c	libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c
Line	598	643
Object	texturedata	texturedata

Code Snippet

File Name	libsdl-org@@SDL-prerelease-2.29.1-CVE-2022-4743-FP.c
Method	static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.      GLES_TextureData *texturedata = NULL;
....
643.              *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=123
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c in line 605 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c in line 605.

	Source	Destination
File	libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c	libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c
Line	610	656
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
610.        GLES_TextureData *texturedata = NULL;
....
656.                    *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=124
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c in line 605 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c in line 605.

	Source	Destination
File	libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c	libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c
Line	610	655
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-release-2.0.18-CVE-2022-4743-TP.c
Method GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
610.        GLES_TextureData *texturedata = NULL;
....
655.                    *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=125

Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c	libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c
Line	598	644
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c
Method static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.      GLES_TextureData *texturedata = NULL;
....
644.               *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=126
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c	libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c
Line	598	643
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-release-2.28.4-CVE-2022-4743-FP.c
Method static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.      GLES_TextureData *texturedata = NULL;
....
643.               *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=127
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c	libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c
Line	598	644
Object	texturedata	texturedata

Code Snippet

File Name	libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c
Method	static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.        GLES_TextureData *texturedata = NULL;
....
644.                *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=128
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c	libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c
Line	598	643
Object	texturedata	texturedata

Code Snippet

File Name	libsdl-org@@SDL-release-2.30.3-CVE-2022-4743-FP.c
Method	static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.        GLES_TextureData *texturedata = NULL;
....
643.                *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=129
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c	libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c
Line	598	644
Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c
Method static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.        GLES_TextureData *texturedata = NULL;
....
644.                *(verts++) = uv_[1] * texturedata->texh;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=130
Status	New

The variable declared in texturedata at libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c in line 593 is not initialized when it is used by texturedata at libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c in line 593.

	Source	Destination
File	libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c	libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c
Line	598	643

Object	texturedata	texturedata

Code Snippet
File Name libsdl-org@@SDL-release-2.30.6-CVE-2022-4743-FP.c
Method static int GLES_QueueGeometry(SDL_Renderer *renderer, SDL_RenderCommand *cmd, SDL_Texture *texture,

```
....
598.        GLES_TextureData *texturedata = NULL;
....
643.                *(verts++) = uv_[0] * texturedata->texw;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=131
Status	New

The variable declared in varname at libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c in line 161 is not initialized when it is used by varname at libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c in line 161.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c	libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c
Line	168	169
Object	varname	varname

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c
Method static int registerlocalvar (LexState *ls, TString *varname) {

```
....
168.        f->locvars[oldsize++].varname = NULL;
169.      f->locvars[fs->nlocvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=132
Status	New

The variable declared in name at libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c in line 228 is not initialized when it is used by name at libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c in line 228.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2022-	libretro@@RetroArch-v1.9.11-CVE-2022-

	28805-FP.c	28805-FP.c
Line	235	238
Object	name	name

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c
Method static int newupvalue (FuncState *fs, TString *name, expdesc *v) {

```
....
235.       f->upvalues[oldsize++].name = NULL;
....
238.     f->upvalues[fs->nups].name = name;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=133
Status	New

The variable declared in prev at libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c in line 1488 is not initialized when it is used by prev at libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c in line 1147.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c	libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c
Line	1494	1152
Object	prev	prev

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c
Method static void exprstat (LexState *ls) {

```
....
1494.       v.prev = NULL;
```

File Name libretro@@RetroArch-v1.9.11-CVE-2022-28805-FP.c

Method static void assignment (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1152.       nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 46:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=134
Status	New

The variable declared in varname at libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c in line 161 is not initialized when it is used by varname at libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c in line 161.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c	libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c
Line	168	169
Object	varname	varname

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c
Method static int registerlocalvar (LexState *ls, TString *varname) {

```
....
168.       f->locvars[oldsize++].varname = NULL;
169.     f->locvars[fs->nlocvars].varname = varname;
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=135
Status	New

The variable declared in name at libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c in line 228 is not initialized when it is used by name at libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c in line 228.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c	libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c
Line	235	238
Object	name	name

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c
Method static int newupvalue (FuncState *fs, TString *name, expdesc *v) {

```
....
235.       f->upvalues[oldsize++].name = NULL;
....
238.     f->upvalues[fs->nups].name = name;
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=136
Status	New

The variable declared in prev at libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c in line 1488 is not initialized when it is used by prev at libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c in line 1147.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c	libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c
Line	1494	1152
Object	prev	prev

Code Snippet

File Name libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c

Method static void exprstat (LexState *ls) {

```
....
1494.       v.prev = NULL;
```

File Name libretro@@RetroArch-v1.9.6-CVE-2022-28805-FP.c

Method static void assignment (LexState *ls, struct LHS_assign *lh, int nvars) {

```
....
1152.       nv.prev = lh;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=137
Status	New

The variable declared in fbo at libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c in line 318 is not initialized when it is used by driverdata at libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c in line 318.

	Source	Destination
File	libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c	libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c
Line	362	403
Object	fbo	driverdata

Code Snippet

File Name libsdl-org@@SDL-2.0.22-RC1-CVE-2022-4743-TP.c

Method GLES_CreateTexture(SDL_Renderer * renderer, SDL_Texture * texture)

```
....
362.            data->fbo = NULL;
....
403.        texture->driverdata = data;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=138
Status	New

The variable declared in fbo at libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c in line 308 is not initialized when it is used by driverdata at libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c in line 308.

	Source	Destination
File	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c
Line	352	393
Object	fbo	driverdata

Code Snippet

File Name	libsdl-org@@SDL-prerelease-2.23.2-CVE-2022-4743-TP.c
Method	GLES_CreateTexture(SDL_Renderer * renderer, SDL_Texture * texture)

```
....
352.            data->fbo = NULL;
....
393.        texture->driverdata = data;
```

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=1020040&projectid=20033&pathid=32
Status	New

The dangerous function, memcpy, was found in use at line 343 in libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	356	356
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method static int read_buf(z_streamp strm, Bytef *buf, unsigned size)

```
....
356.      memcpy(buf, strm->next_in, len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=33
Status	New

The dangerous function, memcpy, was found in use at line 380 in libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	410	410
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method static void fill_window(deflate_state *s)

```
....
410.            memcpy(s->window, s->window+wsize, (unsigned)wsize);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=34
Status	New

The dangerous function, memcpy, was found in use at line 826 in libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	837	837
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method static void flush_pending(z_streamp strm)

```
....
837.     memcpy(strm->next_out, s->pending_out, len);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=35
Status	New

The dangerous function, memcpy, was found in use at line 227 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	234	234
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method static void append_attachment(const uint8_t *data, size_t size)

```
....
234.     memcpy(attachments[attachments_size].data, data, size);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=36

Status	New

The dangerous function, memcpy, was found in use at line 607 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	850	850
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
850.                    memcpy(data, src, width);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=37
Status	New

The dangerous function, memcpy, was found in use at line 607 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	936	936
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
936.                    memcpy(data, src, width);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20

	033&pathid=38
Status	New

The dangerous function, memcpy, was found in use at line 1214 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	1273	1273
Object	memcpy	memcpy

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	static bool open_codecs(void)

```
....
1273.                   memcpy(ass_extra_data[subtitle_streams_num],
(*s)->extradata, size);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=39
Status	New

The dangerous function, memcpy, was found in use at line 227 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	234	234
Object	memcpy	memcpy

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	static void append_attachment(const uint8_t *data, size_t size)

```
....
234.      memcpy(attachments[attachments_size].data, data, size);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=40
Status	New

The dangerous function, memcpy, was found in use at line 607 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	850	850
Object	memcpy	memcpy

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
850.                          memcpy(data, src, width);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=41
Status	New

The dangerous function, memcpy, was found in use at line 607 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	936	936
Object	memcpy	memcpy

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
936.                          memcpy(data, src, width);
```

Dangerous Functions\Path 11:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=42
Status	New

The dangerous function, memcpy, was found in use at line 1214 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	1273	1273
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method static bool open_codecs(void)

```
....
1273.                    memcpy(ass_extra_data[subtitle_streams_num],
(*s)->extradata, size);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=43
Status	New

The dangerous function, memcpy, was found in use at line 343 in libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	356	356
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method static int read_buf(z_streamp strm, Bytef *buf, unsigned size)

```
....
356.     memcpy(buf, strm->next_in, len);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=44
Status	New

The dangerous function, memcpy, was found in use at line 380 in libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	410	410
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method static void fill_window(deflate_state *s)

```
....
410.            memcpy(s->window, s->window+wsize, (unsigned)wsize);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=45
Status	New

The dangerous function, memcpy, was found in use at line 826 in libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	837	837
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method static void flush_pending(z_streamp strm)

```
....
837.     memcpy(strm->next_out, s->pending_out, len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=46
Status	New

The dangerous function, memcpy, was found in use at line 227 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	234	234
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method static void append_attachment(const uint8_t *data, size_t size)

```
....
234.      memcpy(attachments[attachments_size].data, data, size);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=47
Status	New

The dangerous function, memcpy, was found in use at line 607 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	850	850
Object	memcpy	memcpy

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
850.                        memcpy(data, src, width);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=48
Status	New

The dangerous function, memcpy, was found in use at line 607 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	936	936
Object	memcpy	memcpy

Code Snippet	
File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
936.                        memcpy(data, src, width);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=49
Status	New

The dangerous function, memcpy, was found in use at line 1214 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	1273	1273
Object	memcpy	memcpy

Code Snippet	
File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c

Method	static bool open_codecs(void)

```
....
1273.                    memcpy(ass_extra_data[subtitle_streams_num],
(*s)->extradata, size);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=50
Status	New

The dangerous function, memcpy, was found in use at line 42 in llvm@@llvm-project-llvmorg-10.0.0-rc4-CVE-2022-32234-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	llvm@@llvm-project-llvmorg-10.0.0-rc4-CVE-2022-32234-TP.c	llvm@@llvm-project-llvmorg-10.0.0-rc4-CVE-2022-32234-TP.c
Line	57	57
Object	memcpy	memcpy

Code Snippet	
File Name	llvm@@llvm-project-llvmorg-10.0.0-rc4-CVE-2022-32234-TP.c
Method	void SmallVectorBase::grow_pod(void *FirstEl, size_t MinCapacity,

```
....
57.       memcpy(NewElts, this->BeginX, size() * TSize);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=51
Status	New

The dangerous function, memcpy, was found in use at line 42 in llvm@@llvm-project-llvmorg-10.0.1-rc2-CVE-2022-32234-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	llvm@@llvm-project-llvmorg-10.0.1-rc2-CVE-2022-32234-TP.c	llvm@@llvm-project-llvmorg-10.0.1-rc2-CVE-2022-32234-TP.c
Line	57	57
Object	memcpy	memcpy

Code Snippet

File Name	llvm@@llvm-project-llvmorg-10.0.1-rc2-CVE-2022-32234-TP.c
Method	void SmallVectorBase::grow_pod(void *FirstEl, size_t MinCapacity,

```
....
57.       memcpy(NewElts, this->BeginX, size() * TSize);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=52
Status	New

The dangerous function, sscanf, was found in use at line 380 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	413	413
Object	sscanf	sscanf

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	static void check_variables(bool firststart)

```
....
413.         if (sscanf(fft_var.value, "%ux%u", &w, &h) == 2)
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=53
Status	New

The dangerous function, sscanf, was found in use at line 380 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	413	413
Object	sscanf	sscanf

Code Snippet	
File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	static void check_variables(bool firststart)

```
....
413.        if (sscanf(fft_var.value, "%ux%u", &w, &h) == 2)
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=54
Status	New

The dangerous function, sscanf, was found in use at line 380 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	413	413
Object	sscanf	sscanf

Code Snippet	
File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method	static void check_variables(bool firststart)

```
....
413.        if (sscanf(fft_var.value, "%ux%u", &w, &h) == 2)
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=55
Status	New

The dangerous function, strlen, was found in use at line 1709 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	1902	1902

Object	strlen	strlen

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method static void decode_thread(void *data)

```
....
1902.                         sub.rects[i]->ass, strlen(sub.rects[i]-
>ass));
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=56
Status	New

The dangerous function, strlen, was found in use at line 1709 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	1902	1902
Object	strlen	strlen

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method static void decode_thread(void *data)

```
....
1902.                         sub.rects[i]->ass, strlen(sub.rects[i]-
>ass));
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=57
Status	New

The dangerous function, strlen, was found in use at line 1709 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-	libretro@@RetroArch-v1.9.6-CVE-2024-

	23775-TP.c	23775-TP.c
Line	1902	1902
Object	strlen	strlen

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method static void decode_thread(void *data)

```
....
1902.                     sub.rects[i]->ass, strlen(sub.rects[i]-
>ass));
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=58
Status	New

The dangerous function, strlen, was found in use at line 640 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	849	849
Object	strlen	strlen

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method tiffcp(TIFF* in, TIFF* out)

```
....
849.                    int inknameslen = strlen(inknames) + 1;
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=59
Status	New

The dangerous function, strlen, was found in use at line 640 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	854	854
Object	strlen	strlen

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method	tiffcp(TIFF* in, TIFF* out)

```
....
854.                                             inknameslen += (strlen(cp)
+ 1);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=60
Status	New

The dangerous function, strlen, was found in use at line 295 in lua@@lua-v5.4.0-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	lua@@lua-v5.4.0-CVE-2021-3520-FP.c	lua@@lua-v5.4.0-CVE-2021-3520-FP.c
Line	308	308
Object	strlen	strlen

Code Snippet

File Name	lua@@lua-v5.4.0-CVE-2021-3520-FP.c
Method	static void setpath (lua_State *L, const char *fieldname,

```
....
308.       size_t len = strlen(path);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=61
Status	New

The dangerous function, vsnprintf, was found in use at line 214 in libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	221	221
Object	vsnprintf	vsnprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	static void ass_msg_cb(int level, const char *fmt, va_list args, void *data)

```
....
221.            vsnprintf(buffer, sizeof(buffer), fmt, args);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=62
Status	New

The dangerous function, vsnprintf, was found in use at line 214 in libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	221	221
Object	vsnprintf	vsnprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	static void ass_msg_cb(int level, const char *fmt, va_list args, void *data)

```
....
221.            vsnprintf(buffer, sizeof(buffer), fmt, args);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=63
Status	New

The dangerous function, vsnprintf, was found in use at line 214 in libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	221	221
Object	vsnprintf	vsnprintf

Code Snippet

File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c

Method static void ass_msg_cb(int level, const char *fmt, va_list args, void *data)

```
....
221.         vsnprintf(buffer, sizeof(buffer), fmt, args);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=64
Status	New

The dangerous function, atoi, was found in use at line 206 in libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	215	215
Object	atoi	atoi

Code Snippet

File Name libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c

Method processCompressOptions(char* opt)

```
....
215.                        quality = atoi(cp+1);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=65
Status	New

The dangerous function, atoi, was found in use at line 206 in libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	227	227
Object	atoi	atoi

Code Snippet
File Name libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Method processCompressOptions(char* opt)

```
....
227.                            defpredictor = atoi(cp+1);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=66
Status	New

The dangerous function, atoi, was found in use at line 206 in libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	232	232
Object	atoi	atoi

Code Snippet
File Name libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Method processCompressOptions(char* opt)

```
....
232.                            defpredictor = atoi(cp+1);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=67
Status	New

The dangerous function, atoi, was found in use at line 356 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	362	362
Object	atoi	atoi

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method processZIPOptions(char* cp)

```
....
362.                          defpredictor = atoi(cp);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=68
Status	New

The dangerous function, atoi, was found in use at line 356 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	364	364
Object	atoi	atoi

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method processZIPOptions(char* cp)

```
....
364.                          defpreset = atoi(++cp);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=69
Status	New

The dangerous function, atoi, was found in use at line 356 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	366	366
Object	atoi	atoi

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method	processZIPOptions(char* cp)

```
....
366.                                subcodec = atoi(++cp);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=70
Status	New

The dangerous function, atoi, was found in use at line 394 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	407	407
Object	atoi	atoi

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method	processCompressOptions(char* opt)

```
....
407.                                quality = atoi(cp+1);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=71
Status	New

The dangerous function, atoi, was found in use at line 394 in libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	423	423
Object	atoi	atoi

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method processCompressOptions(char* opt)

```
....
423.                        defpredictor = atoi(cp+1);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=72
Status	New

The dangerous function, realloc, was found in use at line 741 in LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Line	756	756
Object	realloc	realloc

Code Snippet
File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Method rfbBool sraRgnIteratorNext(sraRectangleIterator* i,sraRect* r)

```
....
756.            i->sPtrs = (sraSpan**)realloc(i->sPtrs, sizeof(sraSpan*)*i-
>ptrSize);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=73
Status	New

The dangerous function, realloc, was found in use at line 741 in LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Line	756	756
Object	realloc	realloc

Code Snippet
File Name LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Method rfbBool sraRgnIteratorNext(sraRectangleIterator* i,sraRect* r)

```
....
756.          i->sPtrs = (sraSpan**)realloc(i->sPtrs, sizeof(sraSpan*)*i->ptrSize);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=74
Status	New

The dangerous function, atoi, was found in use at line 32 in litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c
Line	38	38
Object	atoi	atoi

Code Snippet
File Name litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
38.       if (env && atoi(env))
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=75

Status	New

The dangerous function, atoi, was found in use at line 32 in litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c
Line	38	38
Object	atoi	atoi

Code Snippet

File Name	litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c
Method	qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
38.       if (env && atoi(env))
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=76
Status	New

The dangerous function, atoi, was found in use at line 37 in litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c
Line	43	43
Object	atoi	atoi

Code Snippet

File Name	litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c
Method	qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
43.       if (env && atoi(env))
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20

	033&pathid=77
Status	New

The dangerous function, atoi, was found in use at line 39 in litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c
Line	45	45
Object	atoi	atoi

Code Snippet
File Name litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
45.       if (env && atoi(env))
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=78
Status	New

The dangerous function, atoi, was found in use at line 39 in litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c
Line	45	45
Object	atoi	atoi

Code Snippet
File Name litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
45.       if (env && atoi(env))
```

Dangerous Functions\Path 48:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=79
Status	New

The dangerous function, atoi, was found in use at line 39 in litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c
Line	45	45
Object	atoi	atoi

Code Snippet
File Name litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
45.       if (env && atoi(env))
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=80
Status	New

The dangerous function, atoi, was found in use at line 39 in litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c
Line	45	45
Object	atoi	atoi

Code Snippet
File Name litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
45.       if (env && atoi(env))
```

Buffer Overflow boundcpy WrongSizeParam

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow boundcpy WrongSizeParam Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow boundcpy WrongSizeParam\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=8
Status	New

The size of the buffer used by elf_parse in Elf_Binary_t, at line 62 of lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that elf_parse passes to Elf_Binary_t, at line 62 of lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c, to overwrite the target buffer.

	Source	Destination
File	lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c
Line	70	70
Object	Elf_Binary_t	Elf_Binary_t

Code Snippet
File Name lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c
Method Elf_Binary_t* elf_parse(const char *file) {

```
....
70.    memset(c_binary, 0, sizeof(Elf_Binary_t));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=9
Status	New

The size of the buffer used by read_buf in len, at line 343 of libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_buf passes to len, at line 343 of libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	356	356
Object	len	len

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method	static int read_buf(z_streamp strm, Bytef *buf, unsigned size)

```
....
356.     memcpy(buf, strm->next_in, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=10
Status	New

The size of the buffer used by flush_pending in len, at line 826 of libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flush_pending passes to len, at line 826 of libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	837	837
Object	len	len

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method	static void flush_pending(z_streamp strm)

```
....
837.     memcpy(strm->next_out, s->pending_out, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=11
Status	New

The size of the buffer used by append_attachment in size, at line 227 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that append_attachment passes to size, at line 227 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	234	234
Object	size	size

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	static void append_attachment(const uint8_t *data, size_t size)

```
....
234.     memcpy(attachments[attachments_size].data, data, size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=12
Status	New

The size of the buffer used by CORE_PREFIX in width, at line 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CORE_PREFIX passes to width, at line 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	850	850
Object	width	width

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
850.                     memcpy(data, src, width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=13
Status	New

The size of the buffer used by CORE_PREFIX in width, at line 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CORE_PREFIX passes to width, at line 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	936	936
Object	width	width

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
936.                    memcpy(data, src, width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=14
Status	New

The size of the buffer used by append_attachment in size, at line 227 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that append_attachment passes to size, at line 227 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	234	234
Object	size	size

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	static void append_attachment(const uint8_t *data, size_t size)

```
....
234.     memcpy(attachments[attachments_size].data, data, size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=15
Status	New

The size of the buffer used by CORE_PREFIX in width, at line 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CORE_PREFIX passes to width, at line 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	850	850

Object	width	width

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
850.                         memcpy(data, src, width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=16
Status	New

The size of the buffer used by CORE_PREFIX in width, at line 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CORE_PREFIX passes to width, at line 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	936	936
Object	width	width

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
936.                         memcpy(data, src, width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=17
Status	New

The size of the buffer used by read_buf in len, at line 343 of libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that read_buf passes to len, at line 343 of libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c

Line	356	356
Object	len	len

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method static int read_buf(z_streamp strm, Bytef *buf, unsigned size)

```
....
356.      memcpy(buf, strm->next_in, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=18
Status	New

The size of the buffer used by flush_pending in len, at line 826 of libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that flush_pending passes to len, at line 826 of libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	837	837
Object	len	len

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method static void flush_pending(z_streamp strm)

```
....
837.      memcpy(strm->next_out, s->pending_out, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=19
Status	New

The size of the buffer used by append_attachment in size, at line 227 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that append_attachment passes to size, at line 227 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-	libretro@@RetroArch-v1.9.6-CVE-2024-

	23775-TP.c	23775-TP.c
Line	234	234
Object	size	size

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method static void append_attachment(const uint8_t *data, size_t size)

```
....
234.      memcpy(attachments[attachments_size].data, data, size);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=20
Status	New

The size of the buffer used by CORE_PREFIX in width, at line 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CORE_PREFIX passes to width, at line 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	850	850
Object	width	width

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
850.                      memcpy(data, src, width);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=21
Status	New

The size of the buffer used by CORE_PREFIX in width, at line 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that CORE_PREFIX passes to width, at line 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c, to overwrite the target buffer.

	Source	Destination

File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	936	936
Object	width	width

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
936.                    memcpy(data, src, width);
```

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=1020040&projectid=20033&pathid=81
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	306	306
Object	window	window

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
306.       s->window       = (Bytef*)calloc(s->w_size, 2*sizeof(Byte));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=82
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	307	307
Object	prev	prev

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
307.      s->prev          = (Posf*) calloc(s->w_size, sizeof(Pos));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=83
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	308	308
Object	head	head

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
308.      s->head          = (Posf*) calloc(s->hash_size, sizeof(Pos));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=84
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c

Line	314	314
Object	overlay	overlay

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
314.     overlay         = (ushf *)calloc(s->lit_bufsize, sizeof(ush)+2);
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=85
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	306	306
Object	window	window

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
306.     s->window       = (Bytef*)calloc(s->w_size, 2*sizeof(Byte));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=86
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	307	307
Object	prev	prev

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
307.      s->prev         = (Posf*) calloc(s->w_size, sizeof(Pos));
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=87
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	308	308
Object	head	head

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
308.      s->head         = (Posf*) calloc(s->hash_size, sizeof(Pos));
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=88
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	314	314
Object	overlay	overlay

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method	int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
314.      overlay        = (ushf *)calloc(s->lit_bufsize, sizeof(ush)+2);
```

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=1020040&projectid=20033&pathid=25
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	static void seek_frame(int seek_frames)

```
....
543.              seek_frames_capped = (int)(seek_step_time *
media.interpolate_fps);
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=26
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
543.                seek_frames_capped = (int)(seek_step_time *
media.interpolate_fps);
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=27
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 500 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	543	543
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
543.                seek_frames_capped = (int)(seek_step_time *
media.interpolate_fps);
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=28
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 493 of libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c
Line	554	554
Object	AssignExpr	AssignExpr

Code Snippet
File Name libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c
Method LZWDecodeCompat(TIFF* tif, tidata_t op0, tsize_t occ0, tsample_t s)

```
....
554.                NextCode(tif, sp, bp, code, GetNextCodeCompat);
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=29
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 493 of libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c
Line	562	562
Object	AssignExpr	AssignExpr

Code Snippet
File Name libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c
Method LZWDecodeCompat(TIFF* tif, tidata_t op0, tsize_t occ0, tsample_t s)

```
....
562.                       NextCode(tif, sp, bp, code, GetNextCodeCompat);
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=30
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 600 of libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c
Line	674	674
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c
Method	LZWDecodeCompat(TIFF* tif, uint8* op0, tmsize_t occ0, uint16 s)

```
....
674.            NextCode(tif, sp, bp, code, GetNextCodeCompat);
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=31
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 600 of libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c
Line	685	685
Object	AssignExpr	AssignExpr

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c
Method	LZWDecodeCompat(TIFF* tif, uint8* op0, tmsize_t occ0, uint16 s)

```
....
685.                    NextCode(tif, sp, bp, code,
GetNextCodeCompat);
```

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=1020040&projectid=20033&pathid=3
Status	New

The application performs an illegal operation in uv__idna_toascii_label, in libuv@@libuv-v1.35.0-CVE-2021-22918-TP.c. In line 102, the program attempts to divide by BinaryExpr, 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 BinaryExpr in uv__idna_toascii_label of libuv@@libuv-v1.35.0-CVE-2021-22918-TP.c, at line 102.

	Source	Destination
File	libuv@@libuv-v1.35.0-CVE-2021-22918-TP.c	libuv@@libuv-v1.35.0-CVE-2021-22918-TP.c
Line	236	236
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name libuv@@libuv-v1.35.0-CVE-2021-22918-TP.c
Method static int uv__idna_toascii_label(const char* s, const char* se,

```
....
236.        bias += 36 * delta / (delta + 38);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=4
Status	New

The application performs an illegal operation in uv__idna_toascii_label, in libuv@@libuv-v1.38.1-CVE-2021-22918-TP.c. In line 102, the program attempts to divide by BinaryExpr, 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 BinaryExpr in uv__idna_toascii_label of libuv@@libuv-v1.38.1-CVE-2021-22918-TP.c, at line 102.

	Source	Destination
File	libuv@@libuv-v1.38.1-CVE-2021-22918-TP.c	libuv@@libuv-v1.38.1-CVE-2021-22918-TP.c
Line	236	236
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name libuv@@libuv-v1.38.1-CVE-2021-22918-TP.c
Method static int uv__idna_toascii_label(const char* s, const char* se,

```
....
236.        bias += 36 * delta / (delta + 38);
```

Divide By Zero\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=5
Status	New

The application performs an illegal operation in uv__idna_toascii_label, in libuv@@libuv-v1.41.0-CVE-2021-22918-TP.c. In line 102, the program attempts to divide by BinaryExpr, 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 BinaryExpr in uv__idna_toascii_label of libuv@@libuv-v1.41.0-CVE-2021-22918-TP.c, at line 102.

	Source	Destination
File	libuv@@libuv-v1.41.0-CVE-2021-22918-TP.c	libuv@@libuv-v1.41.0-CVE-2021-22918-TP.c
Line	236	236
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name libuv@@libuv-v1.41.0-CVE-2021-22918-TP.c
Method static int uv__idna_toascii_label(const char* s, const char* se,

```
....
236.            bias += 36 * delta / (delta + 38);
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=6
Status	New

The application performs an illegal operation in LZWEncode, in libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c. In line 721, the program attempts to divide by outcount, 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 outcount in LZWEncode of libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c, at line 721.

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c
Line	844	844
Object	outcount	outcount

Code Snippet
File Name libsdl-org@@libtiff-v3.5.1-CVE-2023-2731-TP.c
Method LZWEncode(TIFF* tif, tidata_t bp, tsize_t cc, tsample_t s)

```
....
844.                                CALCRATIO(sp, rat);
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=7
Status	New

The application performs an illegal operation in LZWEncode, in libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c. In line 899, the program attempts to divide by outcount, 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 outcount in LZWEncode of libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c, at line 899.

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c
Line	1028	1028
Object	outcount	outcount

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-2731-TP.c
Method	LZWEncode(TIFF* tif, uint8* bp, tmsize_t cc, uint16 s)

```
....
1028.                           CALCRATIO(sp, rat);
```

Float Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Float Overflow Version:1

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

Float Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=22
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	873	873

Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts -
frames[0].pts);
```

Float Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=23
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	873	873
Object	AssignExpr	AssignExpr

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts -
frames[0].pts);
```

Float Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=24
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c

Line	873	873
Object	AssignExpr	AssignExpr

Code Snippet
File Name   libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method   void CORE_PREFIX(retro_run)(void)

```
....
873.            mix_factor = (min_pts - frames[0].pts) / (frames[1].pts -
frames[0].pts);
```

Improper Resource Access Authorization

Query Path:
CPP\Cx\CPP Low Visibility\Improper Resource Access Authorization Version:1

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=1020040&projectid=20033&pathid=159
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	1180	1180
Object	fprintf	fprintf

Code Snippet
File Name   libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Method   pickCopyFunc(TIFF* in, TIFF* out, uint16 bitspersample, uint16 samplesperpixel)

```
....
1180.            fprintf(stderr,
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=160
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	1263	1263
Object	fprintf	fprintf

Code Snippet

File Name	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Method	pickCopyFunc(TIFF* in, TIFF* out, uint16 bitspersample, uint16 samplesperpixel)

```
....
1263.       fprintf(stderr, "tiffcp: %s: Don't know how to copy/convert
image.\n",
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=161
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	290	290
Object	fprintf	fprintf

Code Snippet

File Name	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Method	usage(void)

```
....
290.                fprintf(stderr, "%s\n", stuff[i]);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=162
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	1886	1886

Object	fprintf	fprintf

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method	pickCopyFunc(TIFF* in, TIFF* out, uint16 bitspersample, uint16 samplesperpixel)

```
....
1886.            fprintf(stderr,
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=163
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	1900	1900
Object	fprintf	fprintf

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method	pickCopyFunc(TIFF* in, TIFF* out, uint16 bitspersample, uint16 samplesperpixel)

```
....
1900.                fprintf(stderr,
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=164
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	1978	1978
Object	fprintf	fprintf

Code Snippet

File Name	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method	pickCopyFunc(TIFF* in, TIFF* out, uint16 bitspersample, uint16 samplesperpixel)

```
....
1978.        fprintf(stderr, "tiffcp: %s: Don't know how to copy/convert
image.\n",
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=165
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	119	119
Object	fprintf	fprintf

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method static void* limitMalloc(tmsize_t s)

```
....
119.              fprintf(stderr, "                  use -m option to
change limit.\n");
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=166
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	142	142
Object	fprintf	fprintf

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method static int nextSrcImage (TIFF *tif, char **imageSpec)

```
....
142.                           fprintf (stderr,
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=167
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	149	149
Object	fprintf	fprintf

Code Snippet

File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c

Method static int nextSrcImage (TIFF *tif, char **imageSpec)

```
....
149.            fprintf (stderr, "%s%c%d not found!\n",
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=168
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	520	520
Object	fprintf	fprintf

Code Snippet

File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c

Method usage(int code)

```
....
520.        fprintf(out, "%s\n\n", TIFFGetVersion());
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=169
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	522	522
Object	fprintf	fprintf

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method usage(int code)

```
....
522.            fprintf(out, "%s\n", stuff[i]);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=170
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	668	668
Object	fprintf	fprintf

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method tiffcp(TIFF* in, TIFF* out)

```
....
668.                fprintf(stderr, "tiffcp: %s: Can't copy/convert 
subsampled image.\n",
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=171
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c

Line	145	145
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method int main(int argc, char **argv) {

```
....
145.        fprintf(stderr, "Usage: %s <MachO binary>\n", argv[0]);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=172
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	9	9
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
9.    fprintf(stdout, "Binary Name: %s\n", binary->name);
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=173
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	12	12
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c

Method void print_binary(Macho_Binary_t* binary) {

```
....
12.     fprintf(stdout, "Header\n");
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=174
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	13	13
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
13.     fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=175
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	15	15
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
15.     fprintf(stdout, "CPU Type: %s\n",
CPU_TYPES_to_string(header.cpu_type));
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=176
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	17	17
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
17.    fprintf(stdout, "File type: %s\n", 
FILE_TYPES_to_string(header.file_type));
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=177
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	23	23
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
23.    fprintf(stdout, "Commands\n");
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=178

Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	24	24
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
24.    fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=179
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	39	39
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
39.        fprintf(stdout, "content[0..3]: %02x %02x %02x\n",
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=180
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c

Line	44	44
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
44.     fprintf(stdout, "Segments\n");
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=181
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	45	45
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
45.     fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=182
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	72	72
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c

Method void print_binary(Macho_Binary_t* binary) {

```
....
72.         fprintf(stdout, "content[0..3]: %02x %02x %02x\n",
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=183
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	78	78
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
78.     fprintf(stdout, "Sections\n");
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=184
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	79	79
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
79.     fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=185
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	113	113
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
113.         fprintf(stdout, "content[0..3]: %02x %02x %02x\n",
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=186
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	118	118
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
118.     fprintf(stdout, "Symbols\n");
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=187
Status	New

	Source	Destination
File	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Line	119	119
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.13.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
119.     fprintf(stdout, "=======\n");
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=188
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	145	145
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method int main(int argc, char **argv) {

```
....
145.       fprintf(stderr, "Usage: %s <MachO binary>\n", argv[0]);
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=189
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	9	9

Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
9.     fprintf(stdout, "Binary Name: %s\n", binary->name);
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=190
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	12	12
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
12.     fprintf(stdout, "Header\n");
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=191
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	13	13
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
13.    fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=192
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	15	15
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
15.    fprintf(stdout, "CPU Type: %s\n",
CPU_TYPES_to_string(header.cpu_type));
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=193
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	17	17
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
17.    fprintf(stdout, "File type: %s\n",
FILE_TYPES_to_string(header.file_type));
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=194
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	23	23
Object	fprintf	fprintf

Code Snippet

File Name	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method	void print_binary(Macho_Binary_t* binary) {

```
....
23.     fprintf(stdout, "Commands\n");
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=195
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	24	24
Object	fprintf	fprintf

Code Snippet

File Name	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method	void print_binary(Macho_Binary_t* binary) {

```
....
24.     fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=196
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	39	39
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
39.         fprintf(stdout, "content[0..3]: %02x %02x %02x\n",
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=197
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	44	44
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
44.     fprintf(stdout, "Segments\n");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=198
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	45	45

Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
45.     fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=199
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	72	72
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
72.         fprintf(stdout, "content[0..3]: %02x %02x %02x\n",
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=200
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	78	78
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
78.     fprintf(stdout, "Sections\n");
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=201
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	79	79
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
79.     fprintf(stdout, "========\n");
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=202
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	113	113
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
113.        fprintf(stdout, "content[0..3]: %02x %02x %02x\n",
```

Improper Resource Access Authorization\Path 45:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=203
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	118	118
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
118.     fprintf(stdout, "Symbols\n");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=204
Status	New

	Source	Destination
File	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Line	119	119
Object	fprintf	fprintf

Code Snippet
File Name lief-project@@LIEF-0.14.0-CVE-2024-31636-FP.c
Method void print_binary(Macho_Binary_t* binary) {

```
....
119.     fprintf(stdout, "=======\n");
```

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=1020040&projectid=20033&pathid=213
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	static void seek_frame(int seek_frames)

```
....
563.       snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=214
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	692	692
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
692.          snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=215
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Line	714	714
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
714.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=216
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method static void seek_frame(int seek_frames)

```
....
563.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=217
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	692	692
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
692.         snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=218
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Line	714	714
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.1-CVE-2024-23775-TP.c
Method	void CORE_PREFIX(retro_run)(void)

```
....
714.         snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=219
Status	New

The seek_frame method calls the snprintf function, at line 500 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	563	563
Object	snprintf	snprintf

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method	static void seek_frame(int seek_frames)

```
....
563.      snprintf(msg, sizeof(msg), "%02d:%02d:%02d / %02d:%02d:%02d",
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=220
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	692	692
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
692.        snprintf(msg, sizeof(msg), "Audio Track #%d.",
audio_streams_ptr);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=221
Status	New

The CORE_PREFIX method calls the snprintf function, at line 607 of libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.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	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c	libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Line	714	714
Object	snprintf	snprintf

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2024-23775-TP.c
Method void CORE_PREFIX(retro_run)(void)

```
....
714.        snprintf(msg, sizeof(msg), "Subtitle Track #%d.",
subtitle_streams_ptr);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=222
Status	New

The deflateInit2_ method calls the overlay function, at line 236 of libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.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	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c

Line	314	314
Object	overlay	overlay

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
314.     overlay        = (ushf *)calloc(s->lit_bufsize, sizeof(ush)+2);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=223
Status	New

The deflateInit2_ method calls the overlay function, at line 236 of libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.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	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	314	314
Object	overlay	overlay

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
314.     overlay        = (ushf *)calloc(s->lit_bufsize, sizeof(ush)+2);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=224
Status	New

The elf_parse method calls the Pointer function, at line 62 of lief-project@@LIEF-0.15.0-CVE-2024-31636-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	lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c	lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c
Line	69	69
Object	Pointer	Pointer

Code Snippet
File Name lief-project@@LIEF-0.15.0-CVE-2024-31636-FP.c
Method Elf_Binary_t* elf_parse(const char *file) {

```
....
69.    auto* c_binary =
static_cast<Elf_Binary_t*>(malloc(sizeof(Elf_Binary_t)));
```

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=1020040&projectid=20033&pathid=233
Status	New

The variable declared in null at LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c in line 34 is not initialized when it is used by span at LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c in line 81.

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Line	36	82
Object	null	span

Code Snippet
File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Method sraSpanCreate(int start, int end, const sraSpanList *subspan) {

```
....
36.    if (!item) return NULL;
```

File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c

Method sraSpanDestroy(sraSpan *span) {

```
....
82.    if (span->subspan) sraSpanListDestroy(span->subspan);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=234
Status	New

The variable declared in null at LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c in line 34 is not initialized when it is used by span at LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c in line 81.

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Line	36	82
Object	null	span

Code Snippet

File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c

Method sraSpanCreate(int start, int end, const sraSpanList *subspan) {

```
....
36.    if (!item) return NULL;
```

File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c

Method sraSpanDestroy(sraSpan *span) {

```
....
82.    if (span->subspan) sraSpanListDestroy(span->subspan);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=235
Status	New

The variable declared in null at LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c in line 34 is not initialized when it is used by span at LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c in line 81.

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Line	36	82
Object	null	span

Code Snippet

File Name LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c

Method sraSpanCreate(int start, int end, const sraSpanList *subspan) {

```
....
36.    if (!item) return NULL;
```

File Name LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c

Method sraSpanDestroy(sraSpan *span) {

```
....
82.    if (span->subspan) sraSpanListDestroy(span->subspan);
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=236
Status	New

The variable declared in null at LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c in line 34 is not initialized when it is used by span at LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c in line 81.

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Line	36	82
Object	null	span

Code Snippet

File Name LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c

Method sraSpanCreate(int start, int end, const sraSpanList *subspan) {

```
....
36.    if (!item) return NULL;
```

File Name LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c

Method sraSpanDestroy(sraSpan *span) {

```
....
82.     if (span->subspan) sraSpanListDestroy(span->subspan);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=237
Status	New

The variable declared in null at lua@@lua-v5.4.0-CVE-2022-28805-TP.c in line 1661 is not initialized when it is used by l at lua@@lua-v5.4.0-CVE-2022-28805-TP.c in line 550.

	Source	Destination
File	lua@@lua-v5.4.0-CVE-2022-28805-TP.c	lua@@lua-v5.4.0-CVE-2022-28805-TP.c
Line	1666	553
Object	null	l

Code Snippet

File Name lua@@lua-v5.4.0-CVE-2022-28805-TP.c

Method static void test_then_block (LexState *ls, int *escapelist) {

```
....
1666.     TString *jlb = NULL;
```

File Name lua@@lua-v5.4.0-CVE-2022-28805-TP.c

Method static int newlabelentry (LexState *ls, Labellist *l, TString *name,

```
....
553.     luaM_growvector(ls->L, l->arr, n, l->size,
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=238
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by g at libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c

Line	850	850
Object	0	g

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c
Method static int runafewfinalizers (lua_State *L) {

```
....
850.    g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=239
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by strm at libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	257	257
Object	0	strm

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.      strm->opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=240
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c in line 844 is not initialized when it is used by g at libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c in line 844.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c

Line	850	850
Object	0	g

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c
Method static int runafewfinalizers (lua_State *L) {

```
....
850.     g->gcfinnum = (!g->tobefnz) ? 0  /* nothing more to finalize? */
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=241
Status	New

The variable declared in 0 at libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c in line 236 is not initialized when it is used by strm at libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c in line 236.

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	257	257
Object	0	strm

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method int deflateInit2_(z_streamp strm, int level, int method, int windowBits, int memLevel, int strategy,

```
....
257.      strm->opaque = (voidpf)0;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=242
Status	New

The variable declared in 0 at lua@@lua-v5.4.0-CVE-2020-15889-TP.c in line 120 is not initialized when it is used by g at lua@@lua-v5.4.0-CVE-2020-15889-TP.c in line 596.

	Source	Destination
File	lua@@lua-v5.4.0-CVE-2020-15889-TP.c	lua@@lua-v5.4.0-CVE-2020-15889-TP.c

Line	132	599
Object	0	g

Code Snippet
File Name	lua@@lua-v5.4.0-CVE-2020-15889-TP.c
Method	static GCObject **getgclist (GCObject *o) {

```
....
132.        default: lua_assert(0); return 0;
```

File Name	lua@@lua-v5.4.0-CVE-2020-15889-TP.c

Method	static lu_mem propagatemark (global_State *g) {

```
....
599.      g->gray = *getgclist(o);   /* remove from 'gray' list */
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=243
Status	New

The variable declared in 0 at lua@@lua-v5.4.0-CVE-2020-24371-TP.c in line 120 is not initialized when it is used by g at lua@@lua-v5.4.0-CVE-2020-24371-TP.c in line 596.

	Source	Destination
File	lua@@lua-v5.4.0-CVE-2020-24371-TP.c	lua@@lua-v5.4.0-CVE-2020-24371-TP.c
Line	132	599
Object	0	g

Code Snippet
File Name	lua@@lua-v5.4.0-CVE-2020-24371-TP.c
Method	static GCObject **getgclist (GCObject *o) {

```
....
132.        default: lua_assert(0); return 0;
```

File Name	lua@@lua-v5.4.0-CVE-2020-24371-TP.c

Method	static lu_mem propagatemark (global_State *g) {

```
....
599.      g->gray = *getgclist(o);   /* remove from 'gray' list */
```

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=1020040&projectid=20033&pathid=225
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet

File Name libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c

Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                           sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=226
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet

File Name libretro@@RetroArch-v1.9.11-CVE-2020-24371-FP.c

Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=227
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c
Line	493	493
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c
Method static lu_mem traversetable (global_State *g, Table *h) {

```
....
493.                               sizeof(Proto *) * f->sizep +
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=228
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c	libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c
Line	1049	1049
Object	sizeof	sizeof

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2020-24371-FP.c
Method static lu_mem singlestep (lua_State *L) {

```
....
1049.        g->GCmemtrav = g->strt.size * sizeof(GCObject*);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=229
Status	New

	Source	Destination

File	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Line	701	701
Object	sizeof	sizeof

Code Snippet
File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Method sraRectangleIterator *sraRgnGetIterator(sraRegion *s)

```
....
701.    i->sPtrs = (sraSpan**)malloc(sizeof(sraSpan*)*DEFSIZE);
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=230
Status	New

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Line	756	756
Object	sizeof	sizeof

Code Snippet
File Name LibVNC@@libvncserver-LibVNCServer-0.9.13-CVE-2020-14397-FP.c
Method rfbBool sraRgnIteratorNext(sraRectangleIterator* i,sraRect* r)

```
....
756.         i->sPtrs = (sraSpan**)realloc(i->sPtrs, sizeof(sraSpan*)*i-
>ptrSize);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=231
Status	New

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Line	701	701
Object	sizeof	sizeof

Code Snippet

File Name	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Method	sraRectangleIterator *sraRgnGetIterator(sraRegion *s)

```
....
701.     i->sPtrs = (sraSpan**)malloc(sizeof(sraSpan*)*DEFSIZE);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=232
Status	New

	Source	Destination
File	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Line	756	756
Object	sizeof	sizeof

Code Snippet

File Name	LibVNC@@libvncserver-LibVNCServer-0.9.14-CVE-2020-14397-FP.c
Method	rfbBool sraRgnIteratorNext(sraRectangleIterator* i,sraRect* r)

```
....
756.         i->sPtrs = (sraSpan**)realloc(i->sPtrs, sizeof(sraSpan*)*i->ptrSize);
```

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=1020040&projectid=20033&pathid=206
Status	New

Method qeh_write_type at line 32 of litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-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	litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c
Line	40	40
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v2.12.9-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
40.            s = rand() & 3;
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=207
Status	New

Method qeh_write_type at line 32 of litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-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	litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c
Line	40	40
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v2.13.3-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
40.            s = rand() & 3;
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=208
Status	New

Method qeh_write_type at line 37 of litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-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	litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c
Line	45	45
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v2.17.2-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
45.             s = rand() & 3;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=209
Status	New

Method qeh_write_type at line 39 of litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-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	litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c
Line	47	47
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v2.27.0-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
47.             s = rand() & 3;
```

Use of Insufficiently Random Values\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=210
Status	New

Method qeh_write_type at line 39 of litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-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	litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c
Line	47	47
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v2.29.6-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
47.             s = rand() & 3;
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=211
Status	New

Method qeh_write_type at line 39 of litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-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	litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c
Line	47	47
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v3.0.3-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
47.             s = rand() & 3;
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=212
Status	New

Method qeh_write_type at line 39 of litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-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	litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c	litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c
Line	47	47
Object	rand	rand

Code Snippet
File Name litespeedtech@@lsquic-v3.0.4-CVE-2022-30592-TP.c
Method qeh_write_type (struct qpack_enc_hdl *qeh)

```
....
47.             s = rand() & 3;
```

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=1020040&projectid=20033&pathid=244
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	472	472
Object	ins_h	ins_h

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method static void fill_window(deflate_state *s)

```
....
472.                    s->head[s->ins_h] = (Pos)str;
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=245
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Line	575	575
Object	ins_h	ins_h

Code Snippet
File Name libretro@@RetroArch-v1.9.11-CVE-2023-6992-TP.c
Method int deflateSetDictionary (z_streamp strm, const Bytef *dictionary, uInt dictLength)

```
....
575.            s->head[s->ins_h] = (Pos)str;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=246
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Line	472	472
Object	ins_h	ins_h

Code Snippet
File Name libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method static void fill_window(deflate_state *s)

```
....
472.                s->head[s->ins_h] = (Pos)str;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=247
Status	New

	Source	Destination
File	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c

Line	575	575
Object	ins_h	ins_h

Code Snippet

File Name	libretro@@RetroArch-v1.9.6-CVE-2023-6992-TP.c
Method	int deflateSetDictionary (z_streamp strm, const Bytef *dictionary, uInt dictLength)

```
....
575.            s->head[s->ins_h] = (Pos)str;
```

Inconsistent Implementations

Query Path:

CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=1
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Line	85	85
Object	getopt	getopt

Code Snippet

File Name	libsdl-org@@libtiff-v3.5.1-CVE-2023-6228-TP.c
Method	main(int argc, char* argv[])

```
....
85.    while ((c = getopt(argc, argv, "c:f:l:o:p:r:w:aistBLMC")) != -1)
```

Inconsistent Implementations\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020040&projectid=20033&pathid=2
Status	New

	Source	Destination
File	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c	libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Line	206	206

Object	getopt	getopt

Code Snippet
File Name libsdl-org@@libtiff-v4.2.0-CVE-2023-6228-TP.c
Method main(int argc, char* argv[])

```
....
206.         while ((c = getopt(argc, argv,
"m:,:b:c:f:l:o:p:r:w:aistBLMC8xh")) != -1)
```

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=1020040&projectid=20033&pathid=205
Status	New

	Source	Destination
File	lua@@lua-v5.4.0-CVE-2021-3520-FP.c	lua@@lua-v5.4.0-CVE-2021-3520-FP.c
Line	433	433
Object	f	f

Code Snippet
File Name lua@@lua-v5.4.0-CVE-2021-3520-FP.c
Method static int readable (const char *filename) {

```
....
433.    FILE *f = fopen(filename, "r");  /* try to open file */
```

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=1020040&projectid=20033&pathid=248
Status	New

The readable method in lua@@lua-v5.4.0-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	lua@@lua-v5.4.0-CVE-2021-3520-FP.c	lua@@lua-v5.4.0-CVE-2021-3520-FP.c
Line	433	433
Object	fopen	fopen

Code Snippet
File Name lua@@lua-v5.4.0-CVE-2021-3520-FP.c
Method static int readable (const char *filename) {

```
....
433.     FILE *f = fopen(filename, "r");  /* try to open file */
```

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

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```java
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 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

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));
    }
}
```

Float 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;
}
```

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());
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699** **Seven Pernicious Kingdoms (primary)700** **Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

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 Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		

Previous Entry Names	
Change Date	**Previous Entry Name**
2008-04-11	Inconsistent Implementations

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**

```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

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)
```

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

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

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

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--;
               }
            }
        }
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025