vul_files_3 Scan Report

Project Name	vul_files_3
Scan Start	Monday, January 6, 2025 2:17:24 PM
Preset	Checkmarx Default
Scan Time	01h:52m:28s
Lines Of Code Scanned	299789
Files Scanned	129
Report Creation Time	Monday, January 6, 2025 3:59:04 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

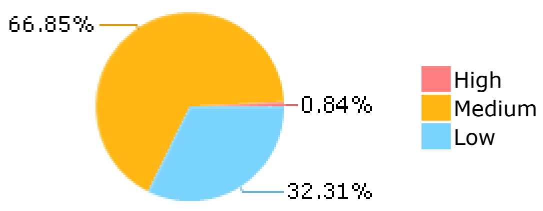
Results Limit

Results limit per query was set to 50

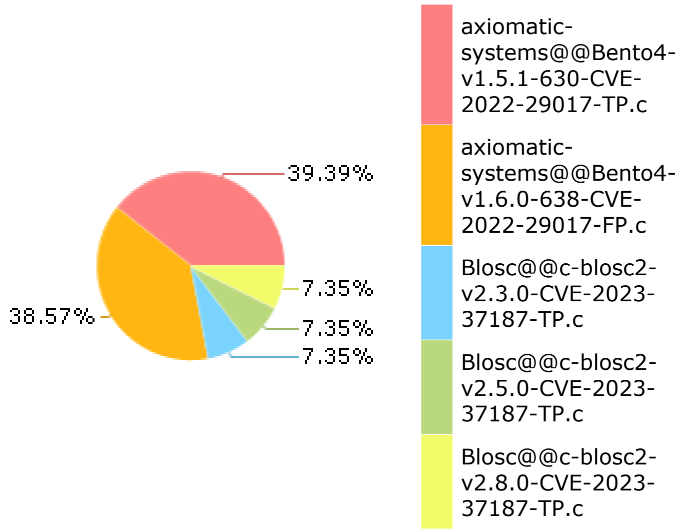
Selected Queries

Selected queries are listed in Result Summary

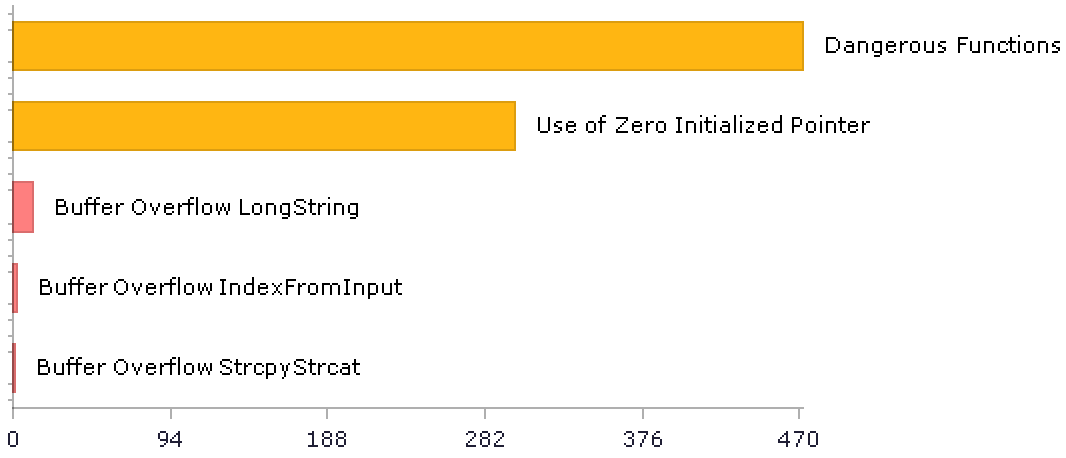
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	250	230
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	250	250
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	11	11
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	472	472
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	7	7
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	472	472
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	246	240
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.	21	21
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.	233	233
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.	12	12

* 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)	250	250
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)	4	4
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)	0	0
SC-4 Information in Shared Resources (P1)	7	7
SC-5 Denial of Service Protection (P1)*****	433	212
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	62	56
SI-11 Error Handling (P2)*****	242	242
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

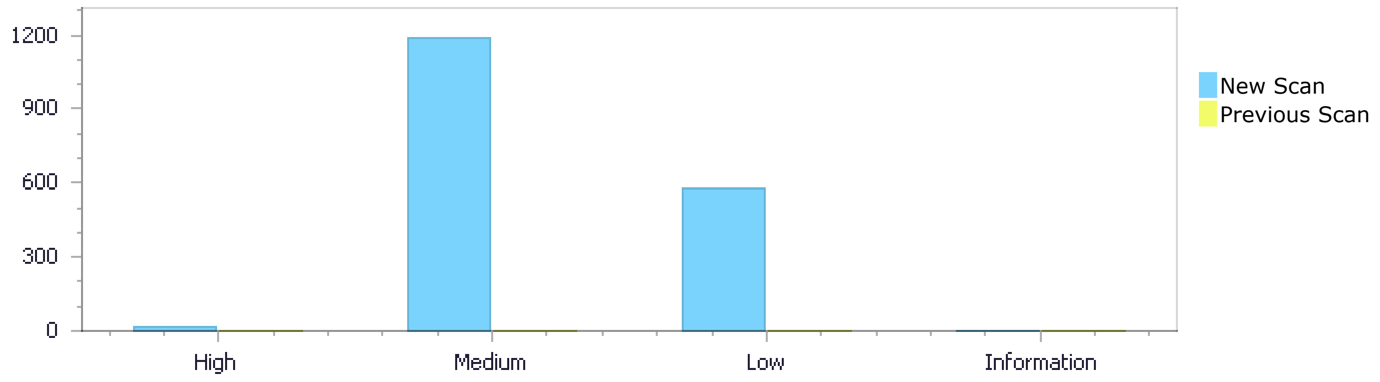
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	15	1,192	576	0	1,783
Recurrent Issues	0	0	0	0	0
Total	15	1,192	576	0	1,783

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	15	1,192	576	0	1,783
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	15	1,192	576	0	1,783

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow LongString	12	High
Buffer Overflow IndexFromInput	2	High
Buffer Overflow StrcpyStrcat	1	High
Dangerous Functions	472	Medium
Use of Zero Initialized Pointer	300	Medium

Buffer Overflow boundcpy WrongSizeParam	212	Medium
Memory Leak	103	Medium
MemoryFree on StackVariable	60	Medium
Integer Overflow	12	Medium
Wrong Size t Allocation	10	Medium
Char Overflow	8	Medium
Heap Inspection	7	Medium
Use of Hard coded Cryptographic Key	4	Medium
Use of Uninitialized Pointer	3	Medium
Buffer Overflow AddressOfLocalVarReturned	1	Medium
Unchecked Return Value	242	Low
Improper Resource Access Authorization	229	Low
Unchecked Array Index	29	Low
NULL Pointer Dereference	22	Low
Incorrect Permission Assignment For Critical Resources	21	Low
TOCTOU	19	Low
Use of Sizeof On a Pointer Type	6	Low
Sizeof Pointer Argument	4	Low
Unreleased Resource Leak	4	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	102
axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	98
atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	27
bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	27
bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	27
bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	27
bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	27
bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	27
bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c	27
bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c	27

Scan Results Details

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 209 of bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 181 of bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Line	183	216
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
183.      static const char * char_to_nibble = "0123456789ABCDEF";
```

File Name bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Method void printf_hexdump(const void *data, int size){

```
....
216.          buffer[0] = char_for_high_nibble(byte);
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=2
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 209 of bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 181 of bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Line	183	217
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
183.      static const char * char_to_nibble = "0123456789ABCDEF";
```

File Name bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Method void printf_hexdump(const void *data, int size){

```
....
217.          buffer[1] = char_for_low_nibble(byte);
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=3
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 211 of bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 183 of bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Line	185	218
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
185.      static const char * char_to_nibble = "0123456789ABCDEF";
```

▼

File Name	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Method	void printf_hexdump(const void * data, int size){

```
....
218.          buffer[0] = char_for_high_nibble(byte);
```

Buffer Overflow LongString\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=4
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 211 of bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 183 of bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Line	185	219
Object	"0123456789ABCDEF"	buffer

Code Snippet

File Name	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Method	char char_for_nibble(int nibble){

```
....
185.      static const char * char_to_nibble = "0123456789ABCDEF";
```

▼

File Name	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Method	void printf_hexdump(const void * data, int size){

```
....
219.          buffer[1] = char_for_low_nibble(byte);
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=5

Status	New

The size of the buffer used by printf_hexdump in buffer, at line 211 of bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 183 of bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Line	185	218
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
185.      static const char * char_to_nibble = "0123456789ABCDEF";
```

File Name bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Method void printf_hexdump(const void * data, int size){

```
....
218.            buffer[0] = char_for_high_nibble(byte);
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=6
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 211 of bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 183 of bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Line	185	219
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
185.      static const char * char_to_nibble = "0123456789ABCDEF";
```

File Name	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Method	void printf_hexdump(const void * data, int size){

```
....
219.          buffer[1] = char_for_low_nibble(byte);
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=7
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 216 of bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 188 of bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Line	190	223
Object	"0123456789ABCDEF"	buffer

Code Snippet

File Name	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Method	char char_for_nibble(int nibble){

```
....
190.      static const char * char_to_nibble = "0123456789ABCDEF";
```

File Name	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Method	void printf_hexdump(const void * data, int size){

```
....
223.          buffer[0] = char_for_high_nibble(byte);
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=8

Status	New

The size of the buffer used by printf_hexdump in buffer, at line 216 of bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 188 of bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Line	190	224
Object	"0123456789ABCDEF"	buffer

Code Snippet

File Name bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c

Method char char_for_nibble(int nibble){

```
....
190.       static const char * char_to_nibble = "0123456789ABCDEF";
```

▼

File Name bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c

Method void printf_hexdump(const void * data, int size){

```
....
224.            buffer[1] = char_for_low_nibble(byte);
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=9
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 223 of bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 195 of bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Line	197	230
Object	"0123456789ABCDEF"	buffer

Code Snippet

File Name bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c

Method char char_for_nibble(int nibble){

```
....
197.       static const char * char_to_nibble = "0123456789ABCDEF";
```

▼

File Name	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Method	void printf_hexdump(const void * data, int size){

```
....
230.           buffer[0] = char_for_high_nibble(byte);
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=10
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 223 of bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 195 of bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Line	197	231
Object	"0123456789ABCDEF"	buffer

Code Snippet

File Name	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Method	char char_for_nibble(int nibble){

```
....
197.       static const char * char_to_nibble = "0123456789ABCDEF";
```

▼

File Name	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Method	void printf_hexdump(const void * data, int size){

```
....
231.           buffer[1] = char_for_low_nibble(byte);
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=11

Status	New

The size of the buffer used by printf_hexdump in buffer, at line 233 of bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 205 of bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Line	207	240
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
207.      static const char * char_to_nibble = "0123456789ABCDEF";
```

File Name bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Method void printf_hexdump(const void * data, int size){

```
....
240.            buffer[0] = char_for_high_nibble(byte);
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=12
Status	New

The size of the buffer used by printf_hexdump in buffer, at line 233 of bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that char_for_nibble passes to "0123456789ABCDEF", at line 205 of bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c, to overwrite the target buffer.

	Source	Destination
File	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Line	207	241
Object	"0123456789ABCDEF"	buffer

Code Snippet
File Name bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Method char char_for_nibble(int nibble){

```
....
207.      static const char * char_to_nibble = "0123456789ABCDEF";
```

▼

File Name bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c

Method void printf_hexdump(const void * data, int size){

```
....
241.          buffer[1] = char_for_low_nibble(byte);
```

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=14
Status	New

The size of the buffer used by SampleEncrypter::EncryptVideoSample in nalu_length_size, at line 519 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1527 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c, to overwrite the target buffer.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1527	548
Object	argv	nalu_length_size

Code Snippet

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method main(int argc, char** argv)

```
....
1527.  main(int argc, char** argv)
```

▼

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method SampleEncrypter::EncryptVideoSample(AP4_DataBuffer& sample, AP4_UI08 nalu_length_size)

```
....
548.          AP4_UI08 nalu_type = nalu[nalu_length_size] & 0x1F;
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=15
Status	New

The size of the buffer used by SampleEncrypter::EncryptVideoSample in nalu_length_size, at line 519 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that main passes to argv, at line 1559 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c, to overwrite the target buffer.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1559	548
Object	argv	nalu_length_size

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	main(int argc, char** argv)

```
....
1559.  main(int argc, char** argv)
```

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	SampleEncrypter::EncryptVideoSample(AP4_DataBuffer& sample, AP4_UI08 nalu_length_size)

```
....
548.          AP4_UI08 nalu_type = nalu[nalu_length_size] & 0x1F;
```

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=13
Status	New

The size of the buffer used by mechlist_build_string in ptr, at line 385 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mechlist_build_string passes to ptr, at line 385 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, to overwrite the target buffer.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	385	395
Object	ptr	ptr

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static void mechlist_build_string(char *ptr, size_t buflen)

```
....
385.  static void mechlist_build_string(char *ptr, size_t buflen)
....
395.              strcpy(ptr, mptr->name);
```

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=1000008&projectid=4&pathid=319
Status	New

The dangerous function, memcpy, was found in use at line 284 in atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	330	330
Object	memcpy	memcpy

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static void sasl_input(sasl_message_t *smsg)

```
....
330.             memcpy(p->p, smsg->buf, len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=320
Status	New

The dangerous function, memcpy, was found in use at line 409 in atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	431	431
Object	memcpy	memcpy

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static void sasl_packet(sasl_session_t *p, char *buf, int len)

```
....
431.             memcpy(mech, buf, len);
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=321
Status	New

The dangerous function, memcpy, was found in use at line 519 in atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	527	527

Object	memcpy	memcpy

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_write(char *target, char *data, int length)

```
....
527.                memcpy(out, data, nbytes);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=322
Status	New

The dangerous function, memcpy, was found in use at line 345 in Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Line	386	386
Object	memcpy	memcpy

Code Snippet

File Name	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Method	static int send_chunk(CONCRETE_IO_HANDLE tls_io, const void* buffer, size_t size, ON_SEND_COMPLETE on_send_complete, void* callback_context)

```
....
386.                        (void)memcpy(out_buffer + sizes.cbHeader,
buffer, size);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=323
Status	New

The dangerous function, memcpy, was found in use at line 475 in Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	Azure@@azure-uamqp-c-newest-CVE-	Azure@@azure-uamqp-c-newest-CVE-

	2024-29195-TP.c	2024-29195-TP.c
Line	482	482
Object	memcpy	memcpy

Code Snippet
File Name Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Method static void on_underlying_io_bytes_received(void* context, const unsigned char* buffer, size_t size)

```
....
482.            (void)memcpy(tls_io_instance->received_bytes +
tls_io_instance->received_byte_count, buffer, size);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=324
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1172	1172
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1172.        memcpy(data.data, cbor_bytestring_handle(auth_data),
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=325
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1173	1173
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=326
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1335	1335
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1335.         memcpy(nonce_base, cbor_bytestring_handle(auth_data),
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=327
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1336	1336
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c

Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.         memcpy(nonce_base+cbor_bytestring_length(auth_data), client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=328
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1619	1619
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1619.        memcpy(data_signed+data_signed_offset, rpid_hash,
rpid_hash_len);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=329
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1622	1622
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1622.        memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=330
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1625	1625
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1625.        memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Dangerous Functions\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=331
Status New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1631	1631
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1631.        memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Dangerous Functions\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=332

Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1634	1634
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1634.         memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=333
Status	New

The dangerous function, memcpy, was found in use at line 1679 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1960	1960
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * register_new_attestation(struct config_module * config, json_t * j_params, json_t * j_scheme_data, json_t * j_credential) {

```
....
1960.               memcpy(cert_x, cbor_bytestring_handle(cbor_value), 
cbor_bytestring_length(cbor_value));
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=334
Status	New

The dangerous function, memcpy, was found in use at line 1679 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1966	1966
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c

Method static json_t * register_new_attestation(struct config_module * config, json_t * j_params, json_t * j_scheme_data, json_t * j_credential) {

```
....
1966.                 memcpy(cert_y, cbor_bytestring_handle(cbor_value), 
cbor_bytestring_length(cbor_value));
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=335
Status	New

The dangerous function, memcpy, was found in use at line 2157 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	2338	2338
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c

Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2338.        memcpy(data_signed, auth_data, auth_data_len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=336
Status	New

The dangerous function, memcpy, was found in use at line 2157 in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	2339	2339
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2339.        memcpy(data_signed+auth_data_len, cdata_hash,
cdata_hash_len);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=337
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1172	1172
Object	memcpy	memcpy

Code Snippet	
File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1172.        memcpy(data.data, cbor_bytestring_handle(auth_data),
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=338
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1173	1173
Object	memcpy	memcpy

Code Snippet	
File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.        memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=339
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1335	1335
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c

Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1335.         memcpy(nonce_base, cbor_bytestring_handle(auth_data),
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=340
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1336	1336
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c

Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.         memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=341
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1619	1619
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1619.         memcpy(data_signed+data_signed_offset, rpid_hash,
rpid_hash_len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=342
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1622	1622
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1622.        memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=343
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1625	1625
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1625.        memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=344
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1631	1631

Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1631.        memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=345
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1634	1634
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1634.        memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=346
Status	New

The dangerous function, memcpy, was found in use at line 1679 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1960	1960
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * register_new_attestation(struct config_module * config, json_t * j_params, json_t * j_scheme_data, json_t * j_credential) {

```
....
1960.                    memcpy(cert_x, cbor_bytestring_handle(cbor_value), 
cbor_bytestring_length(cbor_value));
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=347
Status	New

The dangerous function, memcpy, was found in use at line 1679 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1966	1966
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * register_new_attestation(struct config_module * config, json_t * j_params, json_t * j_scheme_data, json_t * j_credential) {

```
....
1966.                    memcpy(cert_y, cbor_bytestring_handle(cbor_value), 
cbor_bytestring_length(cbor_value));
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=348
Status	New

The dangerous function, memcpy, was found in use at line 2157 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	2338	2338
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c

Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2338.         memcpy(data_signed, auth_data, auth_data_len);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=349
Status	New

The dangerous function, memcpy, was found in use at line 2157 in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	2339	2339
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c

Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2339.         memcpy(data_signed+auth_data_len, cdata_hash, 
cdata_hash_len);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=350
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1172	1172
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1172.         memcpy(data.data, cbor_bytestring_handle(auth_data), 
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=351
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1173	1173
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=352
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1335	1335
Object	memcpy	memcpy

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c

Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1335.         memcpy(nonce_base, cbor_bytestring_handle(auth_data),
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=353
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1336	1336

Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.        memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=354
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1619	1619
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1619.        memcpy(data_signed+data_signed_offset, rpid_hash,
rpid_hash_len);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=355
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1622	1622
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1622.        memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=356
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1625	1625
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1625.        memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=357
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1631	1631
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1631.         memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=358
Status	New

The dangerous function, memcpy, was found in use at line 1518 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1634	1634
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c

Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1634.        memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=359
Status	New

The dangerous function, memcpy, was found in use at line 1679 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1960	1960
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * register_new_attestation(struct config_module * config, json_t * j_params, json_t * j_scheme_data, json_t * j_credential) {

```
....
1960.              memcpy(cert_x, cbor_bytestring_handle(cbor_value),
cbor_bytestring_length(cbor_value));
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=360
Status	New

The dangerous function, memcpy, was found in use at line 1679 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c

Line	1966	1966
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static json_t * register_new_attestation(struct config_module * config, json_t * j_params, json_t * j_scheme_data, json_t * j_credential) {

```
....
1966.                memcpy(cert_y, cbor_bytestring_handle(cbor_value), cbor_bytestring_length(cbor_value));
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=361
Status	New

The dangerous function, memcpy, was found in use at line 2157 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	2338	2338
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2338.          memcpy(data_signed, auth_data, auth_data_len);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=362
Status	New

The dangerous function, memcpy, was found in use at line 2157 in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	2339	2339
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2339.        memcpy(data_signed+auth_data_len, cdata_hash,
cdata_hash_len);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=363
Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1172	1172
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1172.        memcpy(data.data, cbor_bytestring_handle(auth_data),
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=364

Status	New

The dangerous function, memcpy, was found in use at line 1099 in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1173	1173
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data), 
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=365
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1335	1335
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1335.         memcpy(nonce_base, cbor_bytestring_handle(auth_data), 
cbor_bytestring_length(auth_data));
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=366
Status	New

The dangerous function, memcpy, was found in use at line 1276 in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1336	1336
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.        memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=367
Status	New

The dangerous function, memcpy, was found in use at line 1525 in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1626	1626
Object	memcpy	memcpy

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1626.         memcpy(data_signed+data_signed_offset, rpid_hash,
rpid_hash_len);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=368
Status	New

The dangerous function, memcpy, was found in use at line 1525 in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1629	1629
Object	memcpy	memcpy

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1629.         memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

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=1000008&projectid=4&pathid=908

Status	New

The variable declared in block_cipher at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 372 is not initialized when it is used by stream at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 372.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	374	385
Object	block_cipher	stream

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	EncryptingStream::Create(const AP4_UI08* key, const AP4_UI08* iv, AP4_ByteStream* output, EncryptingStream*& stream) {

```
....
374.        AP4_BlockCipher* block_cipher = NULL;
....
385.        stream = new EncryptingStream(stream_cipher, output);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=909
Status	New

The variable declared in input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1839	1889
Object	input	input

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1839.       AP4_ByteStream* input = NULL;
....
1889.           input->Release();
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=910
Status	New

The variable declared in input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1839	2191
Object	input	input

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1839.       AP4_ByteStream* input = NULL;
....
2191.       input->Release();
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=911
Status	New

The variable declared in input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by linear_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1839	1910
Object	input	linear_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1839.      AP4_ByteStream* input = NULL;
....
1910.          linear_reader = new AP4_LinearReader(*movie, input);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=912
Status	New

The variable declared in encryption_key_hex at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1551	1918
Object	encryption_key_hex	video_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1551.      Options.encryption_key_hex                = NULL;
....
1918.              video_reader = new
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=913
Status	New

The variable declared in segment_url_template at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1548	1918

Object	segment_url_template	video_reader

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1548.      Options.segment_url_template          = NULL;
....
1918.               video_reader = new
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=914
Status	New

The variable declared in encryption_key_format_versions at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1556	1918
Object	encryption_key_format_versions	video_reader

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1556.      Options.encryption_key_format_versions = NULL;
....
1918.               video_reader = new
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=915
Status	New

The variable declared in encryption_key_format at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1555	1918
Object	encryption_key_format	video_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1555.      Options.encryption_key_format           = NULL;
....
1918.               video_reader = new
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=916
Status	New

The variable declared in iframe_index_filename at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1546	1918
Object	iframe_index_filename	video_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1546.      Options.iframe_index_filename           = NULL;
....
1918.               video_reader = new
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=917

Status	New

The variable declared in segment_filename_template at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1547	1918
Object	segment_filename_template	video_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1547.      Options.segment_filename_template      = NULL;
....
1918.              video_reader = new 
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=918
Status	New

The variable declared in input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1534	1918
Object	input	video_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1534.      Options.input                          = NULL;
....
1918.              video_reader = new 
FragmentedSampleReader(*linear_reader, video_track->GetId());
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=919
Status	New

The variable declared in encryption_key_format_versions at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1556	1914
Object	encryption_key_format_versions	audio_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1556.       Options.encryption_key_format_versions = NULL;
....
1914.                 audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=920
Status	New

The variable declared in encryption_key_format at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1555	1914
Object	encryption_key_format	audio_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1555.       Options.encryption_key_format           = NULL;
....
1914.                   audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=921
Status	New

The variable declared in iframe_index_filename at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1546	1914
Object	iframe_index_filename	audio_reader

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1546.       Options.iframe_index_filename           = NULL;
....
1914.                   audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=922
Status	New

The variable declared in segment_filename_template at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1547	1914

Object	segment_filename_template	audio_reader

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1547.       Options.segment_filename_template       = NULL;
....
1914.                 audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=923
Status	New

The variable declared in encryption_key_hex at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1551	1914
Object	encryption_key_hex	audio_reader

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1551.       Options.encryption_key_hex              = NULL;
....
1914.                 audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=924
Status	New

The variable declared in segment_url_template at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1548	1914
Object	segment_url_template	audio_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1548.       Options.segment_url_template            = NULL;
....
1914.               audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=925
Status	New

The variable declared in input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_reader at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1534	1914
Object	input	audio_reader

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1534.       Options.input                           = NULL;
....
1914.               audio_reader = new
FragmentedSampleReader(*linear_reader, audio_track->GetId());
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=926

Status	New

The variable declared in input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by input at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1839	1847
Object	input	input

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1839.       AP4_ByteStream* input = NULL;
....
1847.       AP4_File* input_file = new AP4_File(*input, true);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=927
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1898	2117
Object	video_track	video_track

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1898.           video_track = NULL;
....
2117.               double timescale = (double)video_track-
>GetMediaTimeScale();
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=928
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1872	2117
Object	video_track	video_track

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1872.       AP4_Track* video_track = NULL;
....
2117.                double timescale = (double)video_track-
>GetMediaTimeScale();
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=929
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1898	2116
Object	video_track	video_track

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1898.            video_track = NULL;
....
2116.                double media_duration = (double)video_track-
>GetMediaDuration();
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=930
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1872	2116
Object	video_track	video_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1872.       AP4_Track* video_track = NULL;
....
2116.                double media_duration = (double)video_track-
>GetMediaDuration();
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=931
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1898	2115

Object	video_track	video_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1898.           video_track = NULL;
....
2115.               double sample_count = (double)video_track-
>GetSampleCount();
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=932
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1872	2115
Object	video_track	video_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1872.       AP4_Track* video_track = NULL;
....
2115.               double sample_count = (double)video_track-
>GetSampleCount();
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=933
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by chosen_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1898	1061
Object	video_track	chosen_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1898.           video_track = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1061.                       chosen_track = video_track;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=934
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by chosen_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1872	1061
Object	video_track	chosen_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1872.       AP4_Track* video_track = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1061.                         chosen_track = video_track;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=935
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by chosen_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1898	1064
Object	video_track	chosen_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1898.             video_track = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1064.                         chosen_track = video_track;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=936
Status	New

The variable declared in video_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by chosen_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1872	1064
Object	video_track	chosen_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1872.       AP4_Track* video_track = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1064.                   chosen_track = video_track;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=937
Status	New

The variable declared in audio_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by private_extension_data at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1858	1215
Object	audio_track	private_extension_data

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1858.       AP4_Track* audio_track = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1215.                           private_extension_data      =
private_extension_buffer.GetData();
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=938
Status	New

The variable declared in audio_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by chosen_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1858	1055
Object	audio_track	chosen_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1858.       AP4_Track* audio_track = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1055.               chosen_track = audio_track;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=939
Status	New

The variable declared in audio_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1858	1938
Object	audio_track	audio_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1858.       AP4_Track* audio_track = NULL;
....
1938.           sample_description = audio_track-
>GetSampleDescription(0);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=940
Status	New

The variable declared in output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 253 is not initialized when it is used by playlist at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	255	1308
Object	output	playlist

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method OpenOutput(const char* filename_pattern, unsigned int segment_number)

```
....
255.       AP4_ByteStream* output = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1308.       playlist = OpenOutput(Options.index_filename, 0);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=941
Status	New

The variable declared in output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 253 is not initialized when it is used by playlist at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	255	1434
Object	output	playlist

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method OpenOutput(const char* filename_pattern, unsigned int segment_number)

```
....
255.        AP4_ByteStream* output = NULL;
```

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1434.            playlist = OpenOutput(Options.iframe_index_filename, 0);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=942
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1243
Object	segment_output	segment_output

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                              segment_output = NULL;
....
1243.
*segment_output);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=943
Status	New

The variable declared in encrypting_stream at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1243
Object	encrypting_stream	segment_output

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                      EncryptingStream* encrypting_stream = NULL;
....
1243.
*segment_output);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=944
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination

File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1243
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.       AP4_ByteStream*         segment_output = NULL;
....
1243.
*segment_output);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=945
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1248
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                             segment_output = NULL;
....
1248.
*segment_output);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=946
Status	New

The variable declared in encrypting_stream at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1248
Object	encrypting_stream	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                  EncryptingStream* encrypting_stream = NULL;
....
1248.
*segment_output);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=947
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1248
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.      AP4_ByteStream*         segment_output = NULL;
....
1248.
*segment_output);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=948
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1277
Object	segment_output	segment_output

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                              segment_output = NULL;
....
1277.                 segment_output->Tell(frame_end);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=949
Status	New

The variable declared in encrypting_stream at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1277
Object	encrypting_stream	segment_output

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                     EncryptingStream* encrypting_stream = NULL;
....
1277.                 segment_output->Tell(frame_end);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=950
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1277
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.       AP4_ByteStream*           segment_output = NULL;
....
1277.                 segment_output->Tell(frame_end);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=951
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1269
Object	segment_output	segment_output

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                               segment_output = NULL;
....
1269.                   segment_output->Tell(frame_start);
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=952
Status	New

The variable declared in encrypting_stream at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1269
Object	encrypting_stream	segment_output

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                   EncryptingStream* encrypting_stream = NULL;
....
1269.                   segment_output->Tell(frame_start);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=953
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-	axiomatic-systems@@Bento4-v1.5.1-

	630-CVE-2022-29017-TP.c	630-CVE-2022-29017-TP.c
Line	1023	1269
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.       AP4_ByteStream*         segment_output = NULL;
....
1269.                 segment_output->Tell(frame_start);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=954
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1274
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                         segment_output = NULL;
....
1274.                                                   *segment_output);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=955
Status	New

The variable declared in encrypting_stream at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1274
Object	encrypting_stream	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                   EncryptingStream* encrypting_stream = NULL;
....
1274.                                                    *segment_output);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=956
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1274
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.       AP4_ByteStream*          segment_output = NULL;
....
1274.                                                    *segment_output);
```

Use of Zero Initialized Pointer\Path 50:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=957
Status	New

The variable declared in segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1202
Object	segment_output	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                                  segment_output = NULL;
....
1202.                        ts_writer->WritePMT(*segment_output);
```

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=1000008&projectid=4&pathid=17
Status	New

The size of the buffer used by sasl_input in len, at line 284 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sasl_input passes to len, at line 284 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, to overwrite the target buffer.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	330	330
Object	len	len

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_input(sasl_message_t *smsg)

```
....
330.            memcpy(p->p, smsg->buf, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=18
Status	New

The size of the buffer used by sasl_packet in len, at line 409 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sasl_packet passes to len, at line 409 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, to overwrite the target buffer.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	431	431
Object	len	len

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_packet(sasl_session_t *p, char *buf, int len)

```
....
431.            memcpy(mech, buf, len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=19
Status	New

The size of the buffer used by sasl_write in nbytes, at line 519 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that sasl_write passes to nbytes, at line 519 of atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c, to overwrite the target buffer.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	527	527
Object	nbytes	nbytes

Code Snippet	
File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_write(char *target, char *data, int length)

```
....
527.              memcpy(out, data, nbytes);
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=20
Status	New

The size of the buffer used by check_attestation_packed in client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_packed passes to client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1173	1173
Object	client_data_hash_len	client_data_hash_len

Code Snippet	
File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.        memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=21
Status	New

The size of the buffer used by check_attestation_android_safetynet in client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_android_safetynet passes to client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination

File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1336	1336
Object	client_data_hash_len	client_data_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.         memcpy(nonce_base+cbor_bytestring_length(auth_data), client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=22
Status New

The size of the buffer used by check_attestation_fido_u2f in client_data_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to client_data_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1622	1622
Object	client_data_hash_len	client_data_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1622.         memcpy(data_signed+data_signed_offset, client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=23
Status	New

The size of the buffer used by check_attestation_fido_u2f in credential_id_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to credential_id_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1625	1625
Object	credential_id_len	credential_id_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1625.         memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=24
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_x_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_x_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1631	1631
Object	cert_x_len	cert_x_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1631.        memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=25
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_y_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_y_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1634	1634
Object	cert_y_len	cert_y_len

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1634.        memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=26
Status	New

The size of the buffer used by check_assertion in auth_data_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to auth_data_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	2338	2338

Object	auth_data_len	auth_data_len

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2338.         memcpy(data_signed, auth_data, auth_data_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=27
Status	New

The size of the buffer used by check_assertion in cdata_hash_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to cdata_hash_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	2339	2339
Object	cdata_hash_len	cdata_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2339.         memcpy(data_signed+auth_data_len, cdata_hash,
cdata_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=28
Status	New

The size of the buffer used by check_attestation_packed in client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_packed passes to client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1173	1173
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=29
Status	New

The size of the buffer used by check_attestation_android_safetynet in client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_android_safetynet passes to client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1336	1336
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.         memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=30
Status	New

The size of the buffer used by check_attestation_fido_u2f in rpid_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to rpid_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1619	1619
Object	rpid_hash_len	rpid_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1619.        memcpy(data_signed+data_signed_offset, rpid_hash,
rpid_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=31
Status	New

The size of the buffer used by check_attestation_fido_u2f in client_data_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to client_data_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1622	1622
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c

Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1622.         memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=32
Status	New

The size of the buffer used by check_attestation_fido_u2f in credential_id_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to credential_id_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1625	1625
Object	credential_id_len	credential_id_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1625.         memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=33
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_x_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_x_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1631	1631
Object	cert_x_len	cert_x_len

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1631.          memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=34
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_y_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_y_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1634	1634
Object	cert_y_len	cert_y_len

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1634.          memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=35
Status	New

The size of the buffer used by check_assertion in auth_data_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to auth_data_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	2338	2338
Object	auth_data_len	auth_data_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2338.         memcpy(data_signed, auth_data, auth_data_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=36
Status	New

The size of the buffer used by check_assertion in cdata_hash_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to cdata_hash_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	2339	2339
Object	cdata_hash_len	cdata_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2339.         memcpy(data_signed+auth_data_len, cdata_hash, 
cdata_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=37
Status	New

The size of the buffer used by check_attestation_packed in client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_packed passes to client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1173	1173
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c

Method static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.        memcpy(data.data + cbor_bytestring_length(auth_data), 
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=38
Status	New

The size of the buffer used by check_attestation_android_safetynet in client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_android_safetynet passes to client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1336	1336
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c

Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.        memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=39
Status	New

The size of the buffer used by check_attestation_fido_u2f in client_data_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to client_data_hash_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1622	1622
Object	client_data_hash_len	client_data_hash_len

Code Snippet	
File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1622.        memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=40
Status	New

The size of the buffer used by check_attestation_fido_u2f in credential_id_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to credential_id_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1625	1625
Object	credential_id_len	credential_id_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1625.         memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=41
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_x_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_x_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1631	1631
Object	cert_x_len	cert_x_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1631.         memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=42
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_y_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_y_len, at line 1518 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1634	1634
Object	cert_y_len	cert_y_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1634.        memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=43
Status	New

The size of the buffer used by check_assertion in auth_data_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to auth_data_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	2338	2338
Object	auth_data_len	auth_data_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2338.        memcpy(data_signed, auth_data, auth_data_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=44
Status	New

The size of the buffer used by check_assertion in cdata_hash_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to cdata_hash_len, at line 2157 of babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	2339	2339
Object	cdata_hash_len	cdata_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2339.        memcpy(data_signed+auth_data_len, cdata_hash,
cdata_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=45
Status	New

The size of the buffer used by check_attestation_packed in client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_packed passes to client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1173	1173
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=46
Status	New

The size of the buffer used by check_attestation_android_safetynet in client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_android_safetynet passes to client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1336	1336
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.         memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=47
Status	New

The size of the buffer used by check_attestation_fido_u2f in client_data_hash_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to client_data_hash_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1629	1629
Object	client_data_hash_len	client_data_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1629.         memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=48
Status	New

The size of the buffer used by check_attestation_fido_u2f in credential_id_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to credential_id_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1632	1632
Object	credential_id_len	credential_id_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1632.         memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=49
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_x_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_x_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1638	1638
Object	cert_x_len	cert_x_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1638.        memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=50
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_y_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_y_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1641	1641
Object	cert_y_len	cert_y_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c

Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1641.        memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=51
Status	New

The size of the buffer used by check_assertion in auth_data_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to auth_data_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	2345	2345
Object	auth_data_len	auth_data_len

Code Snippet	
File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2345.        memcpy(data_signed, auth_data, auth_data_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=52
Status	New

The size of the buffer used by check_assertion in cdata_hash_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to cdata_hash_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c

Line	2346	2346
Object	cdata_hash_len	cdata_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2346.         memcpy(data_signed+auth_data_len, cdata_hash,
cdata_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=53
Status	New

The size of the buffer used by check_attestation_packed in client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_packed passes to client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	1173	1173
Object	client_data_hash_len	client_data_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=54
Status	New

The size of the buffer used by check_attestation_android_safetynet in client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_android_safetynet passes to client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	1336	1336
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c

Method static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.         memcpy(nonce_base+cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=55
Status	New

The size of the buffer used by check_attestation_fido_u2f in client_data_hash_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to client_data_hash_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	1629	1629
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1629.        memcpy(data_signed+data_signed_offset, client_data_hash,
client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=56
Status	New

The size of the buffer used by check_attestation_fido_u2f in credential_id_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to credential_id_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	1632	1632
Object	credential_id_len	credential_id_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1632.        memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=57
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_x_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_x_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-	babelouest@@glewlwyd-v2.3.0-CVE-

	2022-27240-TP.c	2022-27240-TP.c
Line	1638	1638
Object	cert_x_len	cert_x_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1638.         memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=58
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_y_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_y_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	1641	1641
Object	cert_y_len	cert_y_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1641.         memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=59

Status	New

The size of the buffer used by check_assertion in auth_data_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to auth_data_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	2345	2345
Object	auth_data_len	auth_data_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2345.        memcpy(data_signed, auth_data, auth_data_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=60
Status	New

The size of the buffer used by check_assertion in cdata_hash_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_assertion passes to cdata_hash_len, at line 2164 of babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	2346	2346
Object	cdata_hash_len	cdata_hash_len

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static int check_assertion(struct config_module * config, json_t * j_params, const char * username, json_t * j_scheme_data, json_t * j_assertion) {

```
....
2346.        memcpy(data_signed+auth_data_len, cdata_hash, 
cdata_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=61
Status	New

The size of the buffer used by check_attestation_packed in client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_packed passes to client_data_hash_len, at line 1099 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1173	1173
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_packed(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data, gnutls_pubkey_t g_key) {

```
....
1173.         memcpy(data.data + cbor_bytestring_length(auth_data),
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=62
Status	New

The size of the buffer used by check_attestation_android_safetynet in client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_android_safetynet passes to client_data_hash_len, at line 1276 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1336	1336
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c

Method	static json_t * check_attestation_android_safetynet(json_t * j_params, cbor_item_t * auth_data, cbor_item_t * att_stmt, const unsigned char * client_data) {

```
....
1336.        memcpy(nonce_base+cbor_bytestring_length(auth_data), 
client_data_hash, client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=63
Status	New

The size of the buffer used by check_attestation_fido_u2f in client_data_hash_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to client_data_hash_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1629	1629
Object	client_data_hash_len	client_data_hash_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1629.        memcpy(data_signed+data_signed_offset, client_data_hash, 
client_data_hash_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=64
Status	New

The size of the buffer used by check_attestation_fido_u2f in credential_id_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to credential_id_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1632	1632
Object	credential_id_len	credential_id_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1632.           memcpy(data_signed+data_signed_offset, credential_id,
credential_id_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=65
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_x_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_x_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1638	1638
Object	cert_x_len	cert_x_len

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1638.           memcpy(data_signed+data_signed_offset, cert_x, cert_x_len);
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=66
Status	New

The size of the buffer used by check_attestation_fido_u2f in cert_y_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that check_attestation_fido_u2f passes to cert_y_len, at line 1525 of babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c, to overwrite the target buffer.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1641	1641
Object	cert_y_len	cert_y_len

Code Snippet

File Name babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1641.         memcpy(data_signed+data_signed_offset, cert_y, cert_y_len);
```

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=1000008&projectid=4&pathid=802
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	603	603
Object	name	name

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c

Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                    char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=803
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.        MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=804
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	603	603
Object	name	name

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                   char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=805
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.        MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=806
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	603	603
Object	name	name

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                   char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=807
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	700	700
Object	ordt	ordt

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.        MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=808
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	603	603
Object	name	name

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                    char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=809
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.        MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=810
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	603	603
Object	name	name

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                        char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=811
Status	New

	Source	Destination

File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.       MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=812
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c
Line	603	603
Object	name	name

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c
Method MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                   char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=813
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c
Line	700	700

Object	ordt	ordt

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c
Method MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.       MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=814
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c
Line	603	603
Object	name	name

Code Snippet
File Name bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c
Method MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=815
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet
File Name bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c

Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.       MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=816
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c
Line	603	603
Object	name	name

Code Snippet

File Name	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                 char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=817
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet

File Name	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c
Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.       MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=818
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c
Line	603	603
Object	name	name

Code Snippet

File Name	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
603.                   char *name = malloc(index_name_length + 1);
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=819
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c
Line	700	700
Object	ordt	ordt

Code Snippet

File Name	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c
Method	MOBI_RET mobi_parse_index(const MOBIData *m, MOBIIndx *indx, const size_t indx_record_number) {

```
....
700.       MOBIOrdt *ordt = calloc(1, sizeof(MOBIOrdt));
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=820
Status	New

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	199	199
Object	p	p

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	sasl_session_t *make_session(const char *uid, server_t *server)

```
....
199.        p = malloc(sizeof(sasl_session_t));
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=821
Status	New

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	201	201
Object	uid	uid

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	sasl_session_t *make_session(const char *uid, server_t *server)

```
....
201.        p->uid = strdup(uid);
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=822
Status	New

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	312	312
Object	buf	buf

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static void sasl_input(sasl_message_t *smsg)

```
....
312.                    p->buf = (char *)malloc(len + 1);
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=823
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	94	94
Object	ordt1	ordt1

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
94.         ordt->ordt1 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt1));
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=824
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c

Line	114	114
Object	ordt2	ordt2

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
114.          ordt->ordt2 = malloc(ordt->offsets_count * sizeof(*ordt->ordt2));
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=825
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	372	372
Object	label	label

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.      indx->entries[entry_number].label = malloc(label_length + 1);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=826
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	436	436
Object	tags	tags

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.            indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=827
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                    indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=828
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	657	657
Object	entries	entries

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
657.                indx->entries = malloc(indx->total_entries_count *
sizeof(MOBIIndexEntry));
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=829
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	94	94
Object	ordt1	ordt1

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
94.          ordt->ordt1 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt1));
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=830
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	114	114
Object	ordt2	ordt2

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
114.            ordt->ordt2 = malloc(ordt->offsets_count * sizeof(*ordt->ordt2));
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=831
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	372	372
Object	label	label

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=832
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	436	436
Object	tags	tags

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.          indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=833
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=834
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	657	657
Object	entries	entries

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
657.                    indx->entries = malloc(indx->total_entries_count *
sizeof(MOBIIndexEntry));
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=835
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	94	94
Object	ordt1	ordt1

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
94.         ordt->ordt1 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt1));
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=836
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	114	114
Object	ordt2	ordt2

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
114.         ordt->ordt2 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt2));
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=837
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	372	372
Object	label	label

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=838
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	436	436
Object	tags	tags

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.            indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=839
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                    indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=840
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	657	657
Object	entries	entries

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
657.                    indx->entries = malloc(indx->total_entries_count *
sizeof(MOBIIndexEntry));
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=841
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	94	94
Object	ordt1	ordt1

Code Snippet

File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c

Method static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
94.          ordt->ordt1 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt1));
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=842
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	114	114
Object	ordt2	ordt2

Code Snippet

File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c

Method static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
114.          ordt->ordt2 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt2));
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=843
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	372	372
Object	label	label

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=844
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	436	436
Object	tags	tags

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.            indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=845
Status	New

	Source	Destination

File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=846
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	657	657
Object	entries	entries

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method MOBI_RET mobi_parse_indx(const MOBIPdbRecord *indx_record, MOBIIndx *indx, MOBITagx *tagx, MOBIOrdt *ordt) {

```
....
657.                indx->entries = malloc(indx->total_entries_count *
sizeof(MOBIIndexEntry));
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=847
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c

Line	94	94
Object	ordt1	ordt1

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
94.          ordt->ordt1 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt1));
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=848
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	114	114
Object	ordt2	ordt2

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_ordt(MOBIBuffer *buf, MOBIOrdt *ordt) {

```
....
114.          ordt->ordt2 = malloc(ordt->offsets_count * sizeof(*ordt-
>ordt2));
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=849
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	372	372
Object	label	label

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=850
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	436	436
Object	tags	tags

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.            indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=851
Status	New

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                    indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=237
Status	New

Calling free() (line 284) on a variable that was not dynamically allocated (line 284) in file atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c may result with a crash.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	341	341
Object	tmpbuf	tmpbuf

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static void sasl_input(sasl_message_t *smsg)

```
....
341.                      free(tmpbuf);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=238
Status	New

Calling free() (line 409) on a variable that was not dynamically allocated (line 409) in file atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c may result with a crash.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c

Line	487	487
Object	out	out

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_packet(sasl_session_t *p, char *buf, int len)

```
....
487.                                free(out);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=239
Status	New

Calling free() (line 409) on a variable that was not dynamically allocated (line 409) in file atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c may result with a crash.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	494	494
Object	out	out

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_packet(sasl_session_t *p, char *buf, int len)

```
....
494.                          free(out);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=240
Status	New

Calling free() (line 409) on a variable that was not dynamically allocated (line 409) in file atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c may result with a crash.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c

Line	513	513
Object	out	out

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_packet(sasl_session_t *p, char *buf, int len)

```
....
513.        free(out);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=241
Status	New

Calling free() (line 331) on a variable that was not dynamically allocated (line 331) in file Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c may result with a crash.

	Source	Destination
File	Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c	Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c
Line	340	340
Object	elem	elem

Code Snippet

File Name	Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c
Method	static void __destroy_json_elements(json_array_t *arr)

```
....
340.                free(elem);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=242
Status	New

Calling free() (line 544) on a variable that was not dynamically allocated (line 544) in file Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c may result with a crash.

	Source	Destination
File	Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c	Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c

Line	553	553
Object	memb	memb

Code Snippet
File Name Barenboim@@json-parser-v1.0.0-CVE-2023-23088-TP.c
Method static void __destroy_json_members(json_object_t *obj)

```
....
553.                  free(memb);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=243
Status New

Calling free() (line 331) on a variable that was not dynamically allocated (line 331) in file Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c may result with a crash.

	Source	Destination
File	Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c	Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c
Line	340	340
Object	elem	elem

Code Snippet
File Name Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c
Method static void __destroy_json_elements(json_array_t *arr)

```
....
340.                  free(elem);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=244
Status New

Calling free() (line 544) on a variable that was not dynamically allocated (line 544) in file Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c may result with a crash.

	Source	Destination
File	Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c	Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c

Line	553	553
Object	memb	memb

Code Snippet
File Name Barenboim@@json-parser-v1.0.1-CVE-2023-23088-TP.c
Method static void __destroy_json_members(json_object_t *obj)

```
....
553.                  free(memb);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=245
Status	New

Calling free() (line 10) on a variable that was not dynamically allocated (line 10) in file Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Line	32	32
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Method int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
32.        free(smeta);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=246
Status	New

Calling free() (line 124) on a variable that was not dynamically allocated (line 124) in file Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c

Line	149	149
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Method	int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
149.        free(smeta);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=247
Status	New

Calling free() (line 218) on a variable that was not dynamically allocated (line 218) in file Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Line	239	239
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Method	int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
239.        free(smeta);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=248
Status	New

Calling free() (line 356) on a variable that was not dynamically allocated (line 356) in file Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c

Line	379	379
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Method int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
379.        free(smeta);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=249
Status	New

Calling free() (line 474) on a variable that was not dynamically allocated (line 474) in file Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Line	496	496
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Method int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
496.        free(smeta);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=250
Status	New

Calling free() (line 604) on a variable that was not dynamically allocated (line 604) in file Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c

Line	629	629
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.1.0-CVE-2023-37187-TP.c
Method int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
629.        free(smeta);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=251
Status	New

Calling free() (line 23) on a variable that was not dynamically allocated (line 23) in file Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Line	46	46
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Method int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
46.     free(smeta);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=252
Status	New

Calling free() (line 145) on a variable that was not dynamically allocated (line 145) in file Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c

Line	171	171
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Method int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
171.     free(smeta);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=253
Status	New

Calling free() (line 240) on a variable that was not dynamically allocated (line 240) in file Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Line	262	262
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Method int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
262.     free(smeta);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=254
Status	New

Calling free() (line 386) on a variable that was not dynamically allocated (line 386) in file Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c

Line	410	410
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Method int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
410.    free(smeta);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=255
Status	New

Calling free() (line 505) on a variable that was not dynamically allocated (line 505) in file Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Line	528	528
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Method int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
528.    free(smeta);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=256
Status	New

Calling free() (line 638) on a variable that was not dynamically allocated (line 638) in file Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c

Line	664	664
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.0-CVE-2023-37187-FP.c
Method int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
664.     free(smeta);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=257
Status	New

Calling free() (line 23) on a variable that was not dynamically allocated (line 23) in file Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Line	46	46
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Method int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
46.     free(smeta);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=258
Status	New

Calling free() (line 145) on a variable that was not dynamically allocated (line 145) in file Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c

Line	171	171
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Method int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
171.     free(smeta);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=259
Status	New

Calling free() (line 240) on a variable that was not dynamically allocated (line 240) in file Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Line	262	262
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Method int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
262.     free(smeta);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=260
Status	New

Calling free() (line 386) on a variable that was not dynamically allocated (line 386) in file Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c

Line	410	410
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Method int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
410.     free(smeta);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=261
Status	New

Calling free() (line 505) on a variable that was not dynamically allocated (line 505) in file Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Line	528	528
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Method int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
528.     free(smeta);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=262
Status	New

Calling free() (line 638) on a variable that was not dynamically allocated (line 638) in file Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c

Line	664	664
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.10.5-CVE-2023-37187-FP.c
Method int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
664.     free(smeta);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=263
Status	New

Calling free() (line 23) on a variable that was not dynamically allocated (line 23) in file Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Line	46	46
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Method int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
46.     free(smeta);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=264
Status	New

Calling free() (line 145) on a variable that was not dynamically allocated (line 145) in file Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c

Line	171	171
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Method int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
171.     free(smeta);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=265
Status	New

Calling free() (line 240) on a variable that was not dynamically allocated (line 240) in file Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Line	262	262
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Method int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
262.     free(smeta);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=266
Status	New

Calling free() (line 386) on a variable that was not dynamically allocated (line 386) in file Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c

Line	410	410
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Method	int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
410.     free(smeta);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=267
Status	New

Calling free() (line 505) on a variable that was not dynamically allocated (line 505) in file Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Line	528	528
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Method	int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
528.     free(smeta);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=268
Status	New

Calling free() (line 638) on a variable that was not dynamically allocated (line 638) in file Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c

Line	664	664
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.13.0-CVE-2023-37187-FP.c
Method	int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
664.    free(smeta);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=269
Status	New

Calling free() (line 20) on a variable that was not dynamically allocated (line 20) in file Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Line	43	43
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Method	int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
43.    free(smeta);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=270
Status	New

Calling free() (line 142) on a variable that was not dynamically allocated (line 142) in file Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c

Line	168	168
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Method int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
168.     free(smeta);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=271
Status	New

Calling free() (line 237) on a variable that was not dynamically allocated (line 237) in file Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Line	259	259
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Method int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
259.     free(smeta);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=272
Status	New

Calling free() (line 383) on a variable that was not dynamically allocated (line 383) in file Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c

Line	407	407
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Method int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
407.    free(smeta);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=273
Status	New

Calling free() (line 502) on a variable that was not dynamically allocated (line 502) in file Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Line	525	525
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Method int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
525.    free(smeta);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=274
Status	New

Calling free() (line 635) on a variable that was not dynamically allocated (line 635) in file Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c	Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c

Line	661	661
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.15.0-CVE-2023-37187-FP.c
Method int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
661.     free(smeta);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=275
Status	New

Calling free() (line 11) on a variable that was not dynamically allocated (line 11) in file Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Line	33	33
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Method int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
33.       free(smeta);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=276
Status	New

Calling free() (line 125) on a variable that was not dynamically allocated (line 125) in file Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c

Line	150	150
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Method int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
150.        free(smeta);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=277
Status	New

Calling free() (line 219) on a variable that was not dynamically allocated (line 219) in file Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Line	240	240
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Method int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
240.        free(smeta);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=278
Status	New

Calling free() (line 357) on a variable that was not dynamically allocated (line 357) in file Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c

Line	380	380
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Method int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
380.        free(smeta);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=279
Status	New

Calling free() (line 475) on a variable that was not dynamically allocated (line 475) in file Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Line	497	497
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Method int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
497.        free(smeta);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=280
Status	New

Calling free() (line 605) on a variable that was not dynamically allocated (line 605) in file Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c

Line	630	630
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.3.0-CVE-2023-37187-TP.c
Method int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
630.        free(smeta);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=281
Status	New

Calling free() (line 18) on a variable that was not dynamically allocated (line 18) in file Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Line	40	40
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Method int zfp_acc_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
40.        free(smeta);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=282
Status	New

Calling free() (line 132) on a variable that was not dynamically allocated (line 132) in file Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c

Line	157	157
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Method int zfp_acc_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
157.        free(smeta);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=283
Status	New

Calling free() (line 226) on a variable that was not dynamically allocated (line 226) in file Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Line	247	247
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Method int zfp_prec_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
247.        free(smeta);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=284
Status	New

Calling free() (line 364) on a variable that was not dynamically allocated (line 364) in file Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c

Line	387	387
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Method int zfp_prec_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
387.        free(smeta);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=285
Status	New

Calling free() (line 482) on a variable that was not dynamically allocated (line 482) in file Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Line	504	504
Object	smeta	smeta

Code Snippet
File Name Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Method int zfp_rate_compress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
504.        free(smeta);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=286
Status	New

Calling free() (line 612) on a variable that was not dynamically allocated (line 612) in file Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c may result with a crash.

	Source	Destination
File	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c

Line	637	637
Object	smeta	smeta

Code Snippet

File Name	Blosc@@c-blosc2-v2.5.0-CVE-2023-37187-TP.c
Method	int zfp_rate_decompress(const uint8_t *input, int32_t input_len, uint8_t *output,

```
....
637.        free(smeta);
```

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=1000008&projectid=4&pathid=307
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.83.14-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.83.14-CVE-2022-0546-FP.c	blender@@blender-v2.83.14-CVE-2022-0546-FP.c
Line	353	353
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.83.14-CVE-2022-0546-FP.c
Method	static int fwritecolrs(FILE *file, int width, int channels, unsigned char *ibufscan, float *fpscan)

```
....
353.          for (beg = j; beg < width; beg += cnt) {
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=308
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.83.14-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.83.14-CVE-2022-0546-FP.c	blender@@blender-v2.83.14-CVE-2022-0546-FP.c
Line	364	364
Object	AssignExpr	AssignExpr

Code Snippet
File Name blender@@blender-v2.83.14-CVE-2022-0546-FP.c
Method static int fwritecolrs(FILE *file, int width, int channels, unsigned char *ibufscan, float *fpscan)

```
....
364.            c2 = j + 1;
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=309
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.83.1-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.83.1-CVE-2022-0546-FP.c	blender@@blender-v2.83.1-CVE-2022-0546-FP.c
Line	353	353
Object	AssignExpr	AssignExpr

Code Snippet
File Name blender@@blender-v2.83.1-CVE-2022-0546-FP.c
Method static int fwritecolrs(FILE *file, int width, int channels, unsigned char *ibufscan, float *fpscan)

```
....
353.          for (beg = j; beg < width; beg += cnt) {
```

Integer Overflow\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=310
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.83.1-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.83.1-CVE-2022-0546-FP.c	blender@@blender-v2.83.1-CVE-2022-0546-FP.c
Line	364	364
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.83.1-CVE-2022-0546-FP.c
Method	static int fwritecolrs(FILE *file, int width, int channels, unsigned char *ibufscan, float *fpscan)

```
....
364.              c2 = j + 1;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=311
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.83.7-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.83.7-CVE-2022-0546-FP.c	blender@@blender-v2.83.7-CVE-2022-0546-FP.c
Line	353	353
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.83.7-CVE-2022-0546-FP.c
Method	static int fwritecolrs(FILE *file, int width, int channels, unsigned char *ibufscan, float *fpscan)

```
....
353.          for (beg = j; beg < width; beg += cnt) {
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=312
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.83.7-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.83.7-CVE-2022-0546-FP.c	blender@@blender-v2.83.7-CVE-2022-0546-FP.c
Line	364	364
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.83.7-CVE-2022-0546-FP.c
Method	static int fwritecolrs(FILE *file, int width, int channels, unsigned char *ibufscan, float *fpscan)

```
....
364.            c2 = j + 1;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=313
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.91.2-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.91.2-CVE-2022-0546-FP.c	blender@@blender-v2.91.2-CVE-2022-0546-FP.c
Line	354	354
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.91.2-CVE-2022-0546-FP.c
Method	static int fwritecolrs(

```
....
354.          for (beg = j; beg < width; beg += cnt) {
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=314
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 311 of blender@@blender-v2.91.2-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.91.2-CVE-2022-0546-FP.c	blender@@blender-v2.91.2-CVE-2022-0546-FP.c
Line	365	365
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.91.2-CVE-2022-0546-FP.c
Method	static int fwritecolrs(

```
....
365.            c2 = j + 1;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=315
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 318 of blender@@blender-v2.93.3-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.93.3-CVE-2022-0546-FP.c	blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Line	361	361
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Method	static int fwritecolrs(

```
....
361.          for (beg = j; beg < width; beg += cnt) {
```

Integer Overflow\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=316
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 318 of blender@@blender-v2.93.3-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v2.93.3-CVE-2022-0546-FP.c	blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Line	372	372
Object	AssignExpr	AssignExpr

Code Snippet
File Name blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Method static int fwritecolrs(

```
....
372.            c2 = j + 1;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=317
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 318 of blender@@blender-v3.0.0-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v3.0.0-CVE-2022-0546-FP.c	blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Line	361	361
Object	AssignExpr	AssignExpr

Code Snippet
File Name blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Method static int fwritecolrs(

```
....
361.          for (beg = j; beg < width; beg += cnt) {
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=318
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 318 of blender@@blender-v3.0.0-CVE-2022-0546-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	blender@@blender-v3.0.0-CVE-2022-0546-FP.c	blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Line	372	372
Object	AssignExpr	AssignExpr

Code Snippet

File Name	blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Method	static int fwritecolrs(

```
....
372.          c2 = j + 1;
```

Wrong Size t Allocation

Query Path:

CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=297
Status	New

The function needed_buffer in Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c at line 345 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Line	378	378
Object	needed_buffer	needed_buffer

Code Snippet

File Name	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Method	static int send_chunk(CONCRETE_IO_HANDLE tls_io, const void* buffer, size_t size, ON_SEND_COMPLETE on_send_complete, void* callback_context)

```
....
378.                      unsigned char* out_buffer = (unsigned
char*)malloc(needed_buffer);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=298
Status	New

The function label_length in bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=299
Status	New

The function label_length in bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=300
Status	New

The function label_length in bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	372	372
Object	label_length	label_length

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=301
Status	New

The function label_length in bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Line	372	372

Object	label_length	label_length

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1533-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=302
Status	New

The function label_length in bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-1987-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=303
Status	New

The function label_length in bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2022-29788-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.      indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=304
Status	New

The function label_length in bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet
File Name bfabiszewski@@libmobi-v0.7-CVE-2022-1533-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.      indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=305
Status	New

The function label_length in bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet

File Name	bfabiszewski@@libmobi-v0.7-CVE-2022-1987-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=306
Status	New

The function label_length in bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c at line 340 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c
Line	372	372
Object	label_length	label_length

Code Snippet

File Name	bfabiszewski@@libmobi-v0.7-CVE-2022-29788-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Char Overflow

Query Path:

CPP\Cx\CPP Integer Overflow\Char Overflow Version:1

Categories

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

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=229
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 628 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	637	637
Object	AssignExpr	AssignExpr

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteAdtsHeader(AP4_ByteStream& output,

```
....
637.        bits[2] = 0x40 | (sampling_frequency_index << 2) |
(channel_configuration >> 2);
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=230
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 628 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	638	638
Object	AssignExpr	AssignExpr

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteAdtsHeader(AP4_ByteStream& output,

```
....
638.      bits[3] = ((channel_configuration&0x3)<<6) | ((frame_size+7)
>> 11);
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=231
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 628 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	639	639
Object	AssignExpr	AssignExpr

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteAdtsHeader(AP4_ByteStream& output,

```
....
639.      bits[4] = ((frame_size+7) >> 3)&0xFF;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=232
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 628 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	637	637
Object	AssignExpr	AssignExpr

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	WriteAdtsHeader(AP4_ByteStream& output,

```
....
637.        bits[2] = 0x40 | (sampling_frequency_index << 2) |
(channel_configuration >> 2);
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=233
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 628 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	638	638
Object	AssignExpr	AssignExpr

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	WriteAdtsHeader(AP4_ByteStream& output,

```
....
638.        bits[3] = ((channel_configuration&0x3)<<6) | ((frame_size+7)
>> 11);
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=234
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 628 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	639	639
Object	AssignExpr	AssignExpr

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteAdtsHeader(AP4_ByteStream& output,

```
....
639.      bits[4] = ((frame_size+7) >> 3)&0xFF;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=235
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 673 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	682	682
Object	AssignExpr	AssignExpr

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteAc4Header(AP4_ByteStream& output,

```
....
682.      bits[4] = (frame_size>>16)&0xFF;
```

Char Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=236
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 673 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	683	683
Object	AssignExpr	AssignExpr

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	WriteAc4Header(AP4_ByteStream& output,

```
....
683.        bits[5] = (frame_size>>8 )&0xFF;
```

Heapsection

Heap Inspection

Query Path:

CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=795
Status	New

Method callback_glewlwyd_user_update_password at line 1855 of babelouest@@glewlwyd-v2.1.0-CVE-2021-45379-TP.c defines j_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to j_password, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-45379-TP.c
Line	1857	1857
Object	j_password	j_password

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
1857.     json_t * j_session, * j_password;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=796
Status	New

Method callback_glewlwyd_user_update_password at line 1999 of babelouest@@glewlwyd-v2.3.0-CVE-2021-45379-TP.c defines j_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to j_password, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-45379-TP.c
Line	2001	2001
Object	j_password	j_password

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2001.     json_t * j_session, * j_password;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=797
Status	New

Method callback_glewlwyd_user_update_password at line 2152 of babelouest@@glewlwyd-v2.4.0-CVE-2021-45379-TP.c defines j_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to j_password, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2021-45379-TP.c
Line	2154	2154
Object	j_password	j_password

Code Snippet

File Name	babelouest@@glewlwyd-v2.4.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2154.     json_t * j_session, * j_password;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=798
Status	New

Method callback_glewlwyd_user_update_password at line 2149 of babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c defines j_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to j_password, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Line	2151	2151
Object	j_password	j_password

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Method int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2151.    json_t * j_session, * j_password, * j_element = NULL;
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=799
Status	New

Method callback_glewlwyd_user_update_password at line 2454 of babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c defines j_password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to j_password, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Line	2456	2456
Object	j_password	j_password

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Method int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2456.    json_t * j_session, * j_password, * j_element = NULL;
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=800

Status	New

Method callback_glewlwyd_user_update_password at line 2149 of babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Line	2153	2153
Object	passwords	passwords

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Method int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2153.     const char ** passwords = NULL;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=801
Status	New

Method callback_glewlwyd_user_update_password at line 2454 of babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c defines passwords, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwords, this variable is never cleared from memory.

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Line	2458	2458
Object	passwords	passwords

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Method int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2458.     const char ** passwords = NULL;
```

Use of Hard coded Cryptographic Key

Query Path:
CPP\Cx\CPP Medium Threat\Use of Hard coded Cryptographic Key Version:0

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

[Description](#)

Use of Hard coded Cryptographic Key\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=791
Status	New

The variable encryption_key_uri at line 1527 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1554	1554
Object	encryption_key_uri	encryption_key_uri

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1554.       Options.encryption_key_uri                 = "key.bin";
```

Use of Hard coded Cryptographic Key\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=792
Status	New

The variable encryption_key_uri at line 1559 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1586	1586
Object	encryption_key_uri	encryption_key_uri

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method main(int argc, char** argv)

```
....
1586.      Options.encryption_key_uri             = "key.bin";
```

Use of Hard coded Cryptographic Key\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=793
Status	New

The variable 16 at line 86 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	86	86
Object	16	encryption_key

Code Snippet

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method AP4_UI08 encryption_key[16];

```
....
86.     AP4_UI08              encryption_key[16];
```

Use of Hard coded Cryptographic Key\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=794
Status	New

The variable 16 at line 86 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c is assigned a hardcoded, literal value. This static value is used as an encryption key.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	86	86
Object	16	encryption_key

Code Snippet

File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c

Method AP4_UI08 encryption_key[16];

```
....
86.       AP4_UI08              encryption_key[16];
```

Use of Uninitialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Pointer Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Use of Uninitialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=905
Status	New

The variable declared in n at atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c in line 172 is not initialized when it is used by data at atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c in line 172.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	175	182
Object	n	data

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method sasl_session_t *find_session(const char *uid)

```
....
175.        mowgli_node_t *n;
....
182.              p = n->data;
```

Use of Uninitialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=906
Status	New

The variable declared in n at atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c in line 353 is not initialized when it is used by data at atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c in line 353.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-	atheme@@atheme-v7.2.11-CVE-2022-

	24976-TP.c	24976-TP.c
Line	355	360
Object	n	data

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static sasl_mechanism_t *find_mechanism(char *name)

```
....
355.        mowgli_node_t *n;
....
360.              mptr = n->data;
```

Use of Uninitialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=907
Status	New

The variable declared in n at atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c in line 385 is not initialized when it is used by n at atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c in line 385.

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	388	392
Object	n	n

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static void mechlist_build_string(char *ptr, size_t buflen)

```
....
388.        mowgli_node_t *n;
....
392.              sasl_mechanism_t *mptr = n->data;
```

Buffer Overflow AddressOfLocalVarReturned

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow AddressOfLocalVarReturned\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=16
Status	New

The pointer tls_server_io_schannel_interface_description at Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c in line 1212 is being used after it has been freed.

	Source	Destination
File	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Line	1214	1214
Object	tls_server_io_schannel_interface_description	tls_server_io_schannel_interface_description

Code Snippet

File Name	Azure@@azure-uamqp-c-newest-CVE-2024-29195-TP.c
Method	const IO_INTERFACE_DESCRIPTION* tls_server_io_get_interface_description(void)

```
....
1214.       return &tls_server_io_schannel_interface_description;
```

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=1000008&projectid=4&pathid=1437
Status	New

The *sasl_get_source_name method calls the snprintf function, at line 755 of atheme@@atheme-v7.2.11-CVE-2022-24976-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	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	762	762
Object	snprintf	snprintf

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static const char *sasl_get_source_name(sourceinfo_t *si)

```
....
762.                snprintf(description, BUFSIZE, "Unknown user on %s
(via SASL)", ssi->sess->server->name);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1438
Status	New

The *sasl_get_source_name method calls the snprintf function, at line 755 of atheme@@atheme-v7.2.11-CVE-2022-24976-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	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	768	768
Object	snprintf	snprintf

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static const char *sasl_get_source_name(sourceinfo_t *si)

```
....
768.                snprintf(result, sizeof result, "<%s:%s>%s",
description, si->sourcedesc, si->smu ? entity(si->smu)->name : "");
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1439
Status	New

The *sasl_get_source_name method calls the snprintf function, at line 755 of atheme@@atheme-v7.2.11-CVE-2022-24976-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	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c

Line	770	770
Object	snprintf	snprintf

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static const char *sasl_get_source_name(sourceinfo_t *si)

```
....
770.                snprintf(result, sizeof result, "<%s>%s", description,
si->smu ? entity(si->smu)->name : "");
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1440
Status	New

The may_impersonate method calls the snprintf function, at line 556 of atheme@@atheme-v7.2.11-CVE-2022-24976-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	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	574	574
Object	snprintf	snprintf

Code Snippet
File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method static bool may_impersonate(myuser_t *source_mu, myuser_t *target_mu)

```
....
574.        snprintf(priv, sizeof(priv), PRIV_IMPERSONATE_CLASS_FMT,
classname);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1441
Status	New

The may_impersonate method calls the snprintf function, at line 556 of atheme@@atheme-v7.2.11-CVE-2022-24976-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	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	580	580
Object	snprintf	snprintf

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static bool may_impersonate(myuser_t *source_mu, myuser_t *target_mu)

```
....
580.         snprintf(priv, sizeof(priv), PRIV_IMPERSONATE_ENTITY_FMT,
entity(target_mu)->name);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1442
Status	New

The OpenOutput method calls the sprintf function, at line 253 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	257	257
Object	sprintf	sprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	OpenOutput(const char* filename_pattern, unsigned int segment_number)

```
....
257.       sprintf(filename, filename_pattern, segment_number);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1443
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1322	1322
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1322.           sprintf(string_buffer, "#EXT-X-VERSION:%d\r\n",
Options.hls_version);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1444
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1330	1330
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1330.       sprintf(string_buffer, "%d\r\n", target_duration);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1445
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1398	1398
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1398.                   sprintf(string_buffer, "#EXTINF:%f,\r\n", 
segment_durations[i]);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1446
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1400	1400
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1400.                   sprintf(string_buffer, "#EXTINF:%u,\r\n", (unsigned 
int)(segment_durations[i]+0.5));
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=1447
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1404	1404
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1404.                 sprintf(string_buffer, "#EXT-X-
BYTERANGE:%d@%lld\r\n", segment_sizes[i], segment_positions[i]);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1448
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1407	1407
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1407.             sprintf(string_buffer, Options.segment_url_template, i);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1449
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1439	1439
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1439.              sprintf(string_buffer, "#EXT-X-VERSION:%d\r\n",
Options.hls_version);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1450
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1446	1446
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1446.          sprintf(string_buffer, "%d\r\n",
iframes_target_duration);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1451
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1481	1481
Object	sprintf	sprintf

Code Snippet
File Name   axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method   WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1481.                 sprintf(string_buffer, "#EXTINF:%f,\r\n",
iframe_durations[i]);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1452
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1483	1483
Object	sprintf	sprintf

Code Snippet
File Name   axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method   WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1483.                sprintf(string_buffer, "#EXT-X-
BYTERANGE:%d@%lld\r\n", iframe_sizes[i], iframe_positions[i]);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1453
Status	New

The WriteSamples method calls the sprintf function, at line 998 of axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1485	1485
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1485.                sprintf(string_buffer, Options.segment_url_template,
iframe_segment_indexes[i]);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1454
Status	New

The OpenOutput method calls the sprintf function, at line 253 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	257	257
Object	sprintf	sprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	OpenOutput(const char* filename_pattern, unsigned int segment_number)

```
....
257.      sprintf(filename, filename_pattern, segment_number);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1455
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1354	1354
Object	sprintf	sprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1354.          sprintf(string_buffer, "#EXT-X-VERSION:%d\r\n",
Options.hls_version);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1456
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1362	1362

Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1362.       sprintf(string_buffer, "%d\r\n", target_duration);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1457
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1430	1430
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1430.             sprintf(string_buffer, "#EXTINF:%f,\r\n",
segment_durations[i]);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1458
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c

Line	1432	1432
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1432.                 sprintf(string_buffer, "#EXTINF:%u,\r\n", (unsigned int)(segment_durations[i]+0.5));
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1459
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1436	1436
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1436.                 sprintf(string_buffer, "#EXT-X-BYTERANGE:%d@%lld\r\n", segment_sizes[i], segment_positions[i]);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1460
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1439	1439
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1439.          sprintf(string_buffer, Options.segment_url_template, i);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1461
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1471	1471
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1471.              sprintf(string_buffer, "#EXT-X-VERSION:%d\r\n",
Options.hls_version);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1462
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1478	1478
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1478.           sprintf(string_buffer, "%d\r\n",
iframes_target_duration);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1463
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1513	1513
Object	sprintf	sprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1513.               sprintf(string_buffer, "#EXTINF:%f,\r\n",
iframe_durations[i]);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1464
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1515	1515
Object	sprintf	sprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1515.                   sprintf(string_buffer, "#EXT-X-
BYTERANGE:%d@%lld\r\n", iframe_sizes[i], iframe_positions[i]);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1465
Status	New

The WriteSamples method calls the sprintf function, at line 1022 of axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-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	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1517	1517
Object	sprintf	sprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1517.                   sprintf(string_buffer, Options.segment_url_template,
iframe_segment_indexes[i]);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=1466
Status	New

The saslserv method calls the text function, at line 45 of atheme@@atheme-v7.2.11-CVE-2022-24976-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	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	63	63
Object	text	text

Code Snippet

File Name atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c

Method static void saslserv(sourceinfo_t *si, int parc, char *parv[])

```
....
63.   text = strtok(NULL, "");
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1467
Status	New

The mobi_buffer_dup8 method calls the Pointer function, at line 402 of bfabiszewski@@libmobi-v0.10-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c
Line	407	407
Object	Pointer	Pointer

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c

Method void mobi_buffer_dup8(uint8_t **val, MOBIBuffer *buf) {

```
....
407.     *val = malloc(sizeof(uint8_t));
```

Unchecked Return Value\Path 32:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1468
Status	New

The mobi_buffer_dup16 method calls the Pointer function, at line 424 of bfabiszewski@@libmobi-v0.10-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c
Line	429	429
Object	Pointer	Pointer

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c
Method	void mobi_buffer_dup16(uint16_t **val, MOBIBuffer *buf) {

```
....
429.        *val = malloc(sizeof(uint16_t));
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1469
Status	New

The mobi_buffer_dup32 method calls the Pointer function, at line 446 of bfabiszewski@@libmobi-v0.10-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c
Line	451	451
Object	Pointer	Pointer

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2021-3751-FP.c
Method	void mobi_buffer_dup32(uint32_t **val, MOBIBuffer *buf) {

```
....
451.        *val = malloc(sizeof(uint32_t));
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1470
Status	New

The mobi_parse_index_entry method calls the label function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-1533-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	372	372
Object	label	label

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1471
Status	New

The mobi_parse_index_entry method calls the tags function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-1533-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	436	436
Object	tags	tags

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method	static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.          indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1472
Status	New

The mobi_parse_index_entry method calls the tagvalues function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-1533-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                  indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1473
Status	New

The mobi_trie_get_inflgroups method calls the infl_strings function, at line 1013 of bfabiszewski@@libmobi-v0.10-CVE-2022-1533-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Line	1040	1040

Object	infl_strings	infl_strings

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1533-TP.c
Method size_t mobi_trie_get_inflgroups(char **infl_strings, MOBITrie * const root, const char *string) {

```
....
1040.                infl_strings[count++] = strdup(infl_string);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1474
Status	New

The mobi_parse_index_entry method calls the label function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-1987-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	372	372
Object	label	label

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.        indx->entries[entry_number].label = malloc(label_length + 1);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1475
Status	New

The mobi_parse_index_entry method calls the tags function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-1987-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	436	436
Object	tags	tags

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.            indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1476
Status	New

The mobi_parse_index_entry method calls the tagvalues function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-1987-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet

File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c

Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.                    indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1477
Status	New

The mobi_trie_get_inflgroups method calls the infl_strings function, at line 1013 of bfabiszewski@@libmobi-v0.10-CVE-2022-1987-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	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Line	1040	1040
Object	infl_strings	infl_strings

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-1987-TP.c
Method size_t mobi_trie_get_inflgroups(char **infl_strings, MOBITrie * const root, const char *string) {

```
....
1040.                 infl_strings[count++] = strdup(infl_string);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1478
Status	New

The mobi_parse_index_entry method calls the label function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-29788-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	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	372	372
Object	label	label

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
372.       indx->entries[entry_number].label = malloc(label_length + 1);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1479
Status	New

The mobi_parse_index_entry method calls the tags function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-29788-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	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	436	436
Object	tags	tags

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
436.            indx->entries[entry_number].tags = malloc(tagx->tags_count
* sizeof(MOBIIndexTag));
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1480
Status	New

The mobi_parse_index_entry method calls the tagvalues function, at line 340 of bfabiszewski@@libmobi-v0.10-CVE-2022-29788-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	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	466	466
Object	tagvalues	tagvalues

Code Snippet
File Name bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method static MOBI_RET mobi_parse_index_entry(MOBIIndx *indx, const MOBIIdxt idxt, const MOBITagx *tagx, const MOBIOrdt *ordt, MOBIBuffer *buf, const size_t curr_number) {

```
....
466.              indx->entries[entry_number].tags[i].tagvalues =
malloc(arr_size);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1481
Status	New

The mobi_trie_get_inflgroups method calls the infl_strings function, at line 1013 of bfabiszewski@@libmobi-v0.10-CVE-2022-29788-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	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Line	1040	1040
Object	infl_strings	infl_strings

Code Snippet

File Name	bfabiszewski@@libmobi-v0.10-CVE-2022-29788-FP.c
Method	size_t mobi_trie_get_inflgroups(char **infl_strings, MOBITrie * const root, const char *string) {

```
....
1040.             infl_strings[count++] = strdup(infl_string);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1482
Status	New

The mobi_buffer_dup8 method calls the Pointer function, at line 414 of bfabiszewski@@libmobi-v0.12-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c
Line	419	419
Object	Pointer	Pointer

Code Snippet	
File Name	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c
Method	void mobi_buffer_dup8(uint8_t **val, MOBIBuffer *buf) {

```
....
419.        *val = malloc(sizeof(uint8_t));
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1483
Status	New

The mobi_buffer_dup16 method calls the Pointer function, at line 436 of bfabiszewski@@libmobi-v0.12-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c
Line	441	441
Object	Pointer	Pointer

Code Snippet	
File Name	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c
Method	void mobi_buffer_dup16(uint16_t **val, MOBIBuffer *buf) {

```
....
441.        *val = malloc(sizeof(uint16_t));
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1484
Status	New

The mobi_buffer_dup32 method calls the Pointer function, at line 458 of bfabiszewski@@libmobi-v0.12-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c
Line	463	463
Object	Pointer	Pointer

Code Snippet

File Name	bfabiszewski@@libmobi-v0.12-CVE-2021-3751-FP.c
Method	void mobi_buffer_dup32(uint32_t **val, MOBIBuffer *buf) {

```
....
463.        *val = malloc(sizeof(uint32_t));
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1485
Status	New

The buffer_dup8 method calls the Pointer function, at line 402 of bfabiszewski@@libmobi-v0.5-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.5-CVE-2021-3751-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2021-3751-TP.c
Line	407	407
Object	Pointer	Pointer

Code Snippet

File Name	bfabiszewski@@libmobi-v0.5-CVE-2021-3751-TP.c
Method	void buffer_dup8(uint8_t **val, MOBIBuffer *buf) {

```
....
407.        *val = malloc(sizeof(uint8_t));
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1486
Status	New

The buffer_dup16 method calls the Pointer function, at line 424 of bfabiszewski@@libmobi-v0.5-CVE-2021-3751-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	bfabiszewski@@libmobi-v0.5-CVE-2021-3751-TP.c	bfabiszewski@@libmobi-v0.5-CVE-2021-3751-TP.c
Line	429	429

Object	Pointer	Pointer

Code Snippet
File Name bfabiszewski@@libmobi-v0.5-CVE-2021-3751-TP.c
Method void buffer_dup16(uint16_t **val, MOBIBuffer *buf) {

```
....
429.        *val = malloc(sizeof(uint16_t));
```

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=1000008&projectid=4&pathid=1208
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.         } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1209
Status	New

	Source	Destination

File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.         } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1210
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.         } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1211
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1212
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1213
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1214
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.         } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1215
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.         } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1216

Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1217
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1218
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c

Line	93	93
Object	cert_content	cert_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1219
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	375	375
Object	file_content	file_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method	int callback_static_compressed_inmemory_website (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
375.                      while ((read_length = fread(file_content,
sizeof(char), offset, f))) {
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1220
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	140	140
Object	buf	buf

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method	static ssize_t callback_static_file_uncompressed_stream(void * cls, uint64_t pos, char * buf, size_t max) {

```
....
140.        return fread (buf, sizeof(char), max, (FILE *)cls);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1221
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Line	93	93
Object	cert_content	cert_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
93.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1222
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Line	94	94
Object	cert_content	cert_content

Code Snippet

File Name	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
94.        } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1223
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	369	369
Object	file_content	file_content

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Method int callback_static_compressed_inmemory_website (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
369.                    while ((read_length = fread(file_content,
sizeof(char), offset, f))) {
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1224
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	140	140
Object	buf	buf

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Method static ssize_t callback_static_file_uncompressed_stream(void * cls, uint64_t pos, char * buf, size_t max) {

```
....
140.      return fread (buf, sizeof(char), max, (FILE *)cls);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1225
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c
Line	94	94
Object	cert_content	cert_content

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
94.         } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1226
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c
Line	95	95
Object	cert_content	cert_content

Code Snippet

File Name babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
95.           } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1227
Status	New

	Source	Destination

File	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c
Line	95	95
Object	cert_content	cert_content

Code Snippet

File Name babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
95.           } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1228
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Line	95	95
Object	cert_content	cert_content

Code Snippet

File Name babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
95.           } else if (fread(cert_content, 1, len, fl) != len) {
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1229
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1570	1570
Object	fprintf	fprintf

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1570.                fprintf(stderr, "ERROR: --hls-version requires a
number\n");
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1230
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1575	1575
Object	fprintf	fprintf

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1575.                fprintf(stderr, "ERROR: --hls-version requires
number > 0\n");
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1231
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1580	1580
Object	fprintf	fprintf

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1580.                   fprintf(stderr, "ERROR: --segment-duration
requires a number\n");
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1232
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1586	1586
Object	fprintf	fprintf

Code Snippet

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method main(int argc, char** argv)

```
....
1586.                   fprintf(stderr, "ERROR: --segment-duration-
threshold requires a number\n");
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1233
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1592	1592
Object	fprintf	fprintf

Code Snippet

File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method main(int argc, char** argv)

```
....
1592.                   fprintf(stderr, "ERROR: --segment-filename-
template requires an argument\n");
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1234
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1598	1598
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1598.                     fprintf(stderr, "ERROR: --segment-url-template
requires an argument\n");
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1235
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1604	1604
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1604.                     fprintf(stderr, "ERROR: --pmt-pid requires a
number\n");
```

Improper Resource Access Authorization\Path 29:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1236
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1610	1610
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1610.                fprintf(stderr, "ERROR: --audio-pid requires a
number\n");
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1237
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1616	1616
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1616.                fprintf(stderr, "ERROR: --video-pid requires a
number\n");
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1238
Status	New

	Source	Destination

File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1622	1622
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1622.                   fprintf(stderr, "ERROR: --audio-track-id requires
a number\n");
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1239
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1628	1628
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1628.                   fprintf(stderr, "ERROR: --audio-format requires
an argument\n");
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1240
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1637	1637

Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1637.                 fprintf(stderr, "ERROR: unknown audio format\n");
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1241
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1642	1642
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1642.                 fprintf(stderr, "ERROR: --video-track-id requires
a number\n");
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1242
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1648	1648
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1648.                   fprintf(stderr, "ERROR: --pcr-offset requires a
number\n");
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1243
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1656	1656
Object	fprintf	fprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1656.                   fprintf(stderr, "ERROR: --index-filename requires
a filename\n");
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1244
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1662	1662
Object	fprintf	fprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1662.                   fprintf(stderr, "ERROR: --iframe-index-filename
requires a filename\n");
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1245
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1670	1670
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1670.                 fprintf(stderr, "ERROR: --encryption-key requires
an argument\n");
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1246
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1676	1676
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1676.                 fprintf(stderr, "ERROR: invalid hex key\n");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=1247
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1684	1684
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1684.                       fprintf(stderr, "ERROR: --encryption-mode
requires an argument\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1248
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1692	1692
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1692.                       fprintf(stderr, "ERROR: unknown encryption
mode\n");
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1249
Status	New

	Source	Destination

File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1698	1698
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1698.                       fprintf(stderr, "ERROR: --encryption-iv-mode
requires an argument\n");
```

Improper Resource Access Authorization\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1250
Status New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1708	1708
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1708.                       fprintf(stderr, "ERROR: unknown encryption IV
mode\n");
```

Improper Resource Access Authorization\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1251
Status New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1714	1714

Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1714.                   fprintf(stderr, "ERROR: --encryption-key-uri
requires an argument\n");
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1252
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1720	1720
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1720.                   fprintf(stderr, "ERROR: --encryption-key-format
requires an argument\n");
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1253
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1726	1726
Object	fprintf	fprintf

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c

Method	main(int argc, char** argv)

```
....
1726.                    fprintf(stderr, "ERROR: --encryption-key-format-
versions requires an argument\n");
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1254
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1732	1732
Object	fprintf	fprintf

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1732.                    fprintf(stderr, "ERROR: --encryption-key-line
requires an argument\n");
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1255
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1739	1739
Object	fprintf	fprintf

Code Snippet	
File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1739.             fprintf(stderr, "ERROR: unexpected argument: %s\n",
arg);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1256
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1746	1746
Object	fprintf	fprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1746.           fprintf(stderr, "ERROR: missing input file name\n");
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1257
Status	New

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1750	1750
Object	fprintf	fprintf

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	main(int argc, char** argv)

```
....
1750.           fprintf(stderr, "ERROR: --encryption-key-line requires --
encryption-key and --encryption-key-mode\n");
```

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=1000008&projectid=4&pathid=1715
Status	New

	Source	Destination
File	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Line	528	528
Object	nbytes	nbytes

Code Snippet

File Name	atheme@@atheme-v7.2.11-CVE-2022-24976-TP.c
Method	static void sasl_write(char *target, char *data, int length)

```
....
528.            out[nbytes] = '\0';
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1716
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	1628	1628
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1628.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1717
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	1628	1628
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1628.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1718
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	1628	1628
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1628.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1719
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1720
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1721
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1722
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1723
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1724
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.         data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1725
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.         data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1726
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Line	2167	2167
Object	index	index

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2167.                passwords[index] = json_string_value(j_element);
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1727
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.         data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1728
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Line	1635	1635
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1635.         data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1729
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Line	2472	2472
Object	index	index

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Method int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2472.                 passwords[index] = json_string_value(j_element);
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1730
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Line	1921	1921
Object	data_signed_offset	data_signed_offset

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1921.           data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1731
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c
Line	1921	1921
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1921.           data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1732
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c
Line	1934	1934
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c

Method static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1934.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1733
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c
Line	1932	1932
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1932.        data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1734
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Line	1932	1932
Object	data_signed_offset	data_signed_offset

Code Snippet

File Name	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Method	static json_t * check_attestation_fido_u2f(json_t * j_params, unsigned char * credential_id, size_t credential_id_len, unsigned char * cert_x, size_t cert_x_len, unsigned char * cert_y, size_t cert_y_len, cbor_item_t * att_stmt, unsigned char * rpid_hash, size_t rpid_hash_len, const unsigned char * client_data) {

```
....
1932.          data_signed[data_signed_offset] = 0x04;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1735
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Line	289	289
Object	j	j

Code Snippet
File Name bluekitchen@@btstack-v1.2.1-CVE-2023-48906-TP.c
Method void log_info_key(const char * name, sm_key_t key){

```
....
289.        buffer[j] = 0;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1736
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Line	291	291
Object	j	j

Code Snippet
File Name bluekitchen@@btstack-v1.4.1-CVE-2023-48906-TP.c
Method void log_info_key(const char * name, sm_key_t key){

```
....
291.        buffer[j] = 0;
```

Unchecked Array Index\Path 23:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1737
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Line	291	291
Object	j	j

Code Snippet
File Name bluekitchen@@btstack-v1.5.0-CVE-2023-48906-TP.c
Method void log_info_key(const char * name, sm_key_t key){

```
....
291.        buffer[j] = 0;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1738
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Line	296	296
Object	j	j

Code Snippet
File Name bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Method void log_info_key(const char * name, sm_key_t key){

```
....
296.        buffer[j] = 0;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1739
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Line	545	545
Object	bytes_to_copy	bytes_to_copy

Code Snippet
File Name   bluekitchen@@btstack-v1.5.3-CVE-2023-48906-TP.c
Method   void btstack_strcpy(char * dst, uint16_t dst_size, const char * src){

```
....
545.        dst[bytes_to_copy] = 0;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1740
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Line	303	303
Object	j	j

Code Snippet
File Name   bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Method   void log_info_key(const char * name, sm_key_t key){

```
....
303.        buffer[j] = 0;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1741
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Line	552	552

Object	bytes_to_copy	bytes_to_copy

Code Snippet
File Name bluekitchen@@btstack-v1.5.4-CVE-2023-48906-TP.c
Method void btstack_strcpy(char * dst, uint16_t dst_size, const char * src){

```
....
552.        dst[bytes_to_copy] = 0;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1742
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Line	313	313
Object	j	j

Code Snippet
File Name bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Method void log_info_key(const char * name, sm_key_t key){

```
....
313.        buffer[j] = 0;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1743
Status	New

	Source	Destination
File	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c	bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Line	562	562
Object	bytes_to_copy	bytes_to_copy

Code Snippet
File Name bluekitchen@@btstack-v1.5.6-CVE-2023-48906-TP.c
Method uint16_t btstack_strcpy(char * dst, uint16_t dst_size, const char * src){

```
....
562.      dst[bytes_to_copy] = 0;
```

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=1000008&projectid=4&pathid=1689
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527 is not initialized when it is used by audio_track at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 1527.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1858	1938
Object	null	audio_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method main(int argc, char** argv)

```
....
1858.      AP4_Track* audio_track = NULL;
....
1938.          sample_description = audio_track-
>GetSampleDescription(0);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1690
Status	New

The variable declared in 0 at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_positions at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1027	1101
Object	0	segment_positions

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1027.       AP4_Position            segment_position = 0;
....
1101.                         segment_positions.Append(segment_position);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1691
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1164
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.       AP4_ByteStream*         segment_output = NULL;
....
1164.                    segment_output->Release();
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1692
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1164
Object	null	segment_output

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                                   segment_output = NULL;
....
1164.                         segment_output->Release();
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1693
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1164
Object	null	segment_output

Code Snippet

File Name	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method	WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                         EncryptingStream* encrypting_stream = NULL;
....
1164.                         segment_output->Release();
```

NULL Pointer Dereference\Path 6:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1694
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1269
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1023.       AP4_ByteStream*         segment_output = NULL;
....
1269.               segment_output->Tell(frame_start);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1695
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1269
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                           segment_output = NULL;
....
1269.               segment_output->Tell(frame_start);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1696
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1269
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1158.                   EncryptingStream* encrypting_stream = NULL;
....
1269.               segment_output->Tell(frame_start);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1697
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1023	1277
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1023.      AP4_ByteStream*        segment_output = NULL;
....
1277.                segment_output->Tell(frame_end);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1698
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1121	1277
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1121.                          segment_output = NULL;
....
1277.                segment_output->Tell(frame_end);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1699
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c in line 998.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c	axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Line	1158	1277
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.5.1-630-CVE-2022-29017-TP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1158.                   EncryptingStream* encrypting_stream = NULL;
....
1277.               segment_output->Tell(frame_end);
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1700
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1559 is not initialized when it is used by audio_track at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1559.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1890	1970
Object	null	audio_track

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method main(int argc, char** argv)

```
....
1890.      AP4_Track* audio_track = NULL;
....
1970.           sample_description = audio_track-
>GetSampleDescription(0);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1701
Status	New

The variable declared in 0 at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_positions at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination

File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1051	1133
Object	0	segment_positions

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1051.       AP4_Position            segment_position = 0;
....
1133.                     segment_positions.Append(segment_position);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1702
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1047	1196
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1047.       AP4_ByteStream*         segment_output = NULL;
....
1196.                 segment_output->Release();
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1703
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1153	1196
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1153.                                   segment_output = NULL;
....
1196.                         segment_output->Release();
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1704
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1190	1196
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1190.                         EncryptingStream* encrypting_stream = NULL;
....
1196.                         segment_output->Release();
```

NULL Pointer Dereference\Path 17:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1705
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1047	1301
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1047.       AP4_ByteStream*         segment_output = NULL;
....
1301.               segment_output->Tell(frame_start);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1706
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1153	1301
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1153.                           segment_output = NULL;
....
1301.               segment_output->Tell(frame_start);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1707
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1190	1301
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1190.                   EncryptingStream* encrypting_stream = NULL;
....
1301.               segment_output->Tell(frame_start);
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1708
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1047	1309
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1047.      AP4_ByteStream*        segment_output = NULL;
....
1309.               segment_output->Tell(frame_end);
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1709
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1153	1309
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter*   ts_writer,

```
....
1153.                           segment_output = NULL;
....
1309.               segment_output->Tell(frame_end);
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1710
Status	New

The variable declared in null at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022 is not initialized when it is used by segment_output at axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c in line 1022.

	Source	Destination
File	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c	axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Line	1190	1309
Object	null	segment_output

Code Snippet
File Name axiomatic-systems@@Bento4-v1.6.0-638-CVE-2022-29017-FP.c
Method WriteSamples(AP4_Mpeg2TsWriter* ts_writer,

```
....
1190.                   EncryptingStream* encrypting_stream = NULL;
....
1309.               segment_output->Tell(frame_end);
```

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=1000008&projectid=4&pathid=1744
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1745
Status	New

	Source	Destination

File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1746
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1747
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1748
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1749
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1750
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Line	84	84
Object	fl	fl

Code Snippet

File Name	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1751
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Line	84	84
Object	fl	fl

Code Snippet

File Name	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1752

Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1753
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1754
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c

Line	84	84
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1755
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	363	363
Object	f	f

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method int callback_static_compressed_inmemory_website (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
363.                      f = fopen (file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1756
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	193	193
Object	f	f

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method	static int callback_static_file_uncompressed (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
193.        f = fopen (file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1757
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Line	84	84
Object	fl	fl

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
84.    fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1758
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Line	85	85
Object	fl	fl

Code Snippet

File Name	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
85.    fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1759
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	357	357
Object	f	f

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c

Method int callback_static_compressed_inmemory_website (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
357.                    f = fopen (file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1760
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	189	189
Object	f	f

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c

Method static int callback_static_file_uncompressed (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
189.        f = fopen (file_path, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 18:

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

	[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1761]()
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c
Line	85	85
Object	fl	fl

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	[http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1762]()
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c
Line	85	85
Object	fl	fl

Code Snippet

File Name babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	[http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1763]()
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.3-CVE-	babelouest@@glewlwyd-v2.7.3-CVE-

	2023-49208-TP.c	2023-49208-TP.c
Line	85	85
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1764
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Line	85	85
Object	fl	fl

Code Snippet
File Name babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

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=1000008&projectid=4&pathid=1765
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination

File	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1766
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1767
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.1.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1768
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1769
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1770
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.3.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1771
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1772
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1773
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.4.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1774
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2021-40818-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1775
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1776
Status	New

The callback_static_file_uncompressed method in babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	193	193
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method static int callback_static_file_uncompressed (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
193.         f = fopen (file_path, "rb");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1777
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Line	84	84
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
84.     fl = fopen(path, "r");
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1778
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Line	85	85
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-27240-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1779
Status	New

The callback_static_file_uncompressed method in babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	189	189
Object	fopen	fopen

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c

Method static int callback_static_file_uncompressed (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
189.       f = fopen (file_path, "rb");
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1780
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c
Line	85	85
Object	fopen	fopen

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2023-49208-TP.c

Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&

	pathid=1781
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c
Line	85	85
Object	fopen	fopen

Code Snippet

File Name	babelouest@@glewlwyd-v2.7.0-CVE-2023-49208-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1782
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c
Line	85	85
Object	fopen	fopen

Code Snippet

File Name	babelouest@@glewlwyd-v2.7.3-CVE-2023-49208-TP.c
Method	static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

TOCTOU\Path 19:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1783
Status	New

The get_cert_from_file_path method in babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c file utilizes fopen that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c	babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Line	85	85
Object	fopen	fopen

Code Snippet
File Name babelouest@@glewlwyd-v2.7.5-CVE-2023-49208-TP.c
Method static json_t * get_cert_from_file_path(const char * path) {

```
....
85.     fl = fopen(path, "r");
```

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=1000008&projectid=4&pathid=1679
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Line	2165	2165
Object	sizeof	sizeof

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Method int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2165.           if ((passwords =
o_malloc(json_array_size(json_object_get(j_password, "password")) *
sizeof(char *))) != NULL) {
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1680
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Line	2185	2185
Object	sizeof	sizeof

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2185.           if ((passwords = o_malloc(sizeof(char *))) != NULL) {
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1681
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	275	275
Object	sizeof	sizeof

Code Snippet

File Name	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method	int u_add_mime_types_compressed(struct _u_compressed_inmemory_website_config * config, const char * mime_type) {

```
....
275.      if ((config->mime_types_compressed = o_realloc(config-
>mime_types_compressed, (config-
>mime_types_compressed_size+2)*sizeof(char*))) != NULL) {
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1682
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Line	2470	2470
Object	sizeof	sizeof

Code Snippet

File Name	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2470.           if ((passwords =
o_malloc(json_array_size(json_object_get(j_password, "password")) *
sizeof(char *))) != NULL) {
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1683
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Line	2490	2490
Object	sizeof	sizeof

Code Snippet

File Name	babelouest@@glewlwyd-v2.6.0-CVE-2021-45379-TP.c
Method	int callback_glewlwyd_user_update_password (const struct _u_request * request, struct _u_response * response, void * user_data) {

```
....
2490.           if ((passwords = o_malloc(sizeof(char *))) != NULL) {
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1684

Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	270	270
Object	sizeof	sizeof

Code Snippet

File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c

Method int u_add_mime_types_compressed(struct _u_compressed_inmemory_website_config * config, const char * mime_type) {

```
....
270.       if ((config->mime_types_compressed = o_realloc(config-
>mime_types_compressed, (config-
>mime_types_compressed_size+2)*sizeof(char*))) != NULL) {
```

Unreleased Resource Leak

Query Path:

CPP\Cx\CPP Low Visibility\Unreleased Resource Leak Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Unreleased Resource Leak\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1685
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	250	250
Object	mutexattr	mutexattr

Code Snippet

File Name babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c

Method int u_init_compressed_inmemory_website_config(struct _u_compressed_inmemory_website_config * config) {

```
....
250.         pthread_mutexattr_init (&mutexattr);
```

Unreleased Resource Leak\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1686
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	245	245
Object	mutexattr	mutexattr

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Method int u_init_compressed_inmemory_website_config(struct _u_compressed_inmemory_website_config * config) {

```
....
245.        pthread_mutexattr_init (&mutexattr);
```

Unreleased Resource Leak\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1687
Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Line	252	252
Object	config	config

Code Snippet
File Name babelouest@@glewlwyd-v2.5.0-CVE-2022-29967-TP.c
Method int u_init_compressed_inmemory_website_config(struct _u_compressed_inmemory_website_config * config) {

```
....
252.        if (pthread_mutex_init(&(config->lock), &mutexattr) != 0) {
```

Unreleased Resource Leak\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1688

Status	New

	Source	Destination
File	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c	babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Line	247	247
Object	config	config

Code Snippet
File Name babelouest@@glewlwyd-v2.6.0-CVE-2022-29967-TP.c
Method int u_init_compressed_inmemory_website_config(struct _u_compressed_inmemory_website_config * config) {

```
....
247.        if (pthread_mutex_init(&(config->lock), &mutexattr) != 0) {
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1711
Status	New

	Source	Destination
File	blender@@blender-v2.93.3-CVE-2022-0546-FP.c	blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Line	287	287
Object	Pointer	sizeof

Code Snippet
File Name blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Method struct ImBuf *imb_loadhdr(const unsigned char *mem,

```
....
287.     sline = (RGBE *)MEM_mallocN(sizeof(*sline) * width, __func__);
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1712
Status	New

	Source	Destination
File	blender@@blender-v2.93.3-CVE-2022-0546-FP.c	blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Line	287	287
Object	Pointer	sizeof

Code Snippet
File Name blender@@blender-v2.93.3-CVE-2022-0546-FP.c
Method struct ImBuf *imb_loadhdr(const unsigned char *mem,

```
....
287.     sline = (RGBE *)MEM_mallocN(sizeof(*sline) * width, __func__);
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1713
Status	New

	Source	Destination
File	blender@@blender-v3.0.0-CVE-2022-0546-FP.c	blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Line	287	287
Object	Pointer	sizeof

Code Snippet
File Name blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Method struct ImBuf *imb_loadhdr(const unsigned char *mem,

```
....
287.     sline = (RGBE *)MEM_mallocN(sizeof(*sline) * width, __func__);
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000008&projectid=4&pathid=1714
Status	New

	Source	Destination
File	blender@@blender-v3.0.0-CVE-2022-0546-FP.c	blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Line	287	287

Object	Pointer	sizeof

Code Snippet
File Name blender@@blender-v3.0.0-CVE-2022-0546-FP.c
Method struct ImBuf *imb_loadhdr(const unsigned char *mem,

```
....
287.    sline = (RGBE *)MEM_mallocN(sizeof(*sline) * width, __func__);
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];
```

```
void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow AddressOfLocalVarReturned

Risk

What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

Cause

How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

General Recommendations

How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

Source Code Examples

CPP

Use of Variable after It was Freed

```
free(input);
printf("%s", input);
```

Use of Pointer to Local Variable That Was Freed On Return

```
int* func1()
{
      int i;
      i = 1;
      return &i;
}

void func2()
```

```
{
      int j;
      j = 5;
}

//..
      int * i = func1();
      printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
      func2();
      printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Char Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```cpp
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```cpp
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
    - Derive the size value from the length of intended source to determine the amount of units to be processed.
    - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
    - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

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;
}
```

Use of Hard coded Cryptographic Key

Risk

What might happen

Static, unchangeable encryption keys in the source code can be stolen by an attacker with access to the source code or the application binaries. Once the attacker has the encryption key, this can be used to gain access to any encrypted secret data, thus violating the confidentiality of the data. Furthermore, it would be impossible to replace the encryption key once stolen. Note that if this is a product that can be installed numerous times, the encryption key will always be the same, allowing an attacker to break all instances at the same cost.

Cause

How does it happen

The application code uses an encryption key to encrypt and decrypt sensitive data. While it is important to create this encryption key randomly and keep it secret, the application has a single, static key embedded in plain text in the source code.

An attacker could gain access to the source code - whether in the source control system, developer workstations, or the server filesystem or product binaries themselves. Once the attacker has gained access to the source code, it is trivial to retrieve the plain text encryption key and use it to decrypt the sensitive data that the application was protecting.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store any sensitive information, such as encryption keys, in plain text.
- Never hardcode encryption keys in the application source code.
- Implement proper key management, including dynamically generating random keys, protecting keys, and replacing keys as necessary.

Specific Recommendations:

- Remove the hardcoded encryption key from the application source code. Instead, retrieve the key from an external, protected store.

Source Code Examples

Java

Common example of hardcoded encryption key

```
//Generate a key
string encryptionKey = "EncryptionKey123"

//Encrypt the data
SecretKeySpec keySpec = new SecretKeySpec(encryptionKey.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
output = cipher.doFinal(input)
```

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;
  void setPassword()
 {
     password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
     byte[] sKey = getKeyFromConfig();
     Cipher c = Cipher.getInstance("AES");
     c.init(Cipher.ENCRYPT_MODE, sKey);

     char[] input = System.console().readPassword("Enter your password: ");
     password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
     printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}
```

```
int main()
{
    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n'){
                   password[i]='\0';
                   break;
            } else{
                   password[i++]=ch;
                   fflush(0);
            }
      }
      i=0;
      memset(password,'\0',256);
}

int main()
{
      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
            if (ch == '\n')
                   break;
      }
}
```

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 Uninitialized 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

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());
```

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

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

Resource Locking Problems

Category ID: 411 *(Category)* **Status:** Draft

Description

Description Summary

Weaknesses in this category are related to improper handling of locks that are used to control access to resources.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	412	Unrestricted Externally Accessible Lock	Development Concepts699
ParentOf	Weakness Base	413	Insufficient Resource Locking	**Development Concepts (primary)699**
ParentOf	Weakness Base	414	Missing Lock Check	**Development Concepts (primary)699**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Resource Locking problems

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		

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

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

Improper 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

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
        public static int counter = 0;
        public static void start() throws InterruptedException {
               incrementCounter ic;
               decrementCounter dc;
               while(counter == 0) {
                      counter = 0;
                      ic = new incrementCounter();
                      dc = new decrementCounter();
                      ic.start();
                      dc.start();
                      ic.join();
                      dc.join();
               }
               System.out.println(counter); //Will stop and return either -1 or 1 due to race
 condition over counter
        }

        public static class incrementCounter extends Thread {
            public void run() {
               counter++;
            }
```

```
}

public static class decrementCounter extends Thread {
    public void run() {
       counter--;
    }
}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
public static int counter = 0;
public static Object lock = new Object();

public static void start() throws InterruptedException {
       incrementCounter ic;
       decrementCounter dc;
       while(counter == 0) { // because of proper locking, this condition is never false
              counter = 0;
              ic = new incrementCounter();
              dc = new decrementCounter();
              ic.start();
              dc.start();
              ic.join();
              dc.join();
       }
       System.out.println(counter); // Never reached
}

public static class incrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter++;
       }
    }
}

public static class decrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter--;
       }
    }
}
```

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025