vul_files_15 Scan Report

Project Name	vul_files_15
Scan Start	Monday, January 6, 2025 8:13:42 PM
Preset	Checkmarx Default
Scan Time	03h:43m:05s
Lines Of Code Scanned	295985
Files Scanned	72
Report Creation Time	Monday, January 6, 2025 10:57:11 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	7/1000 (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

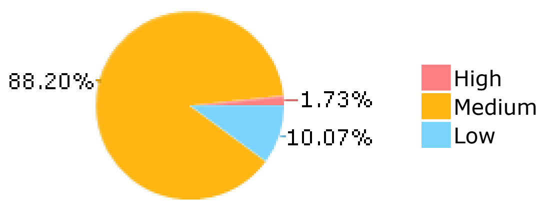
Results Limit

Results limit per query was set to 50

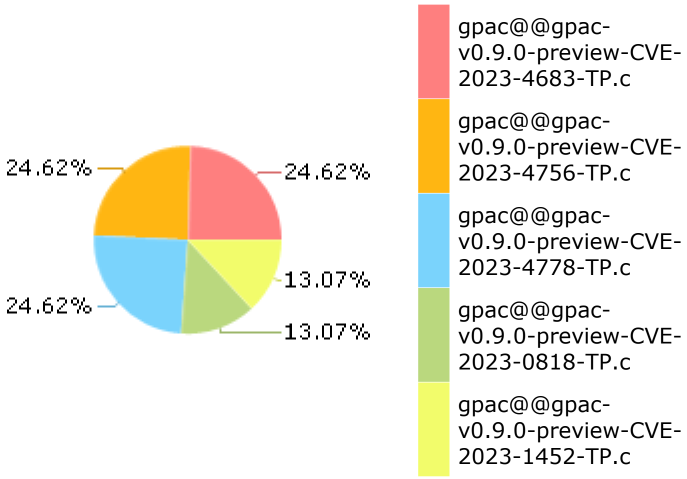
Selected Queries

Selected queries are listed in Result Summary

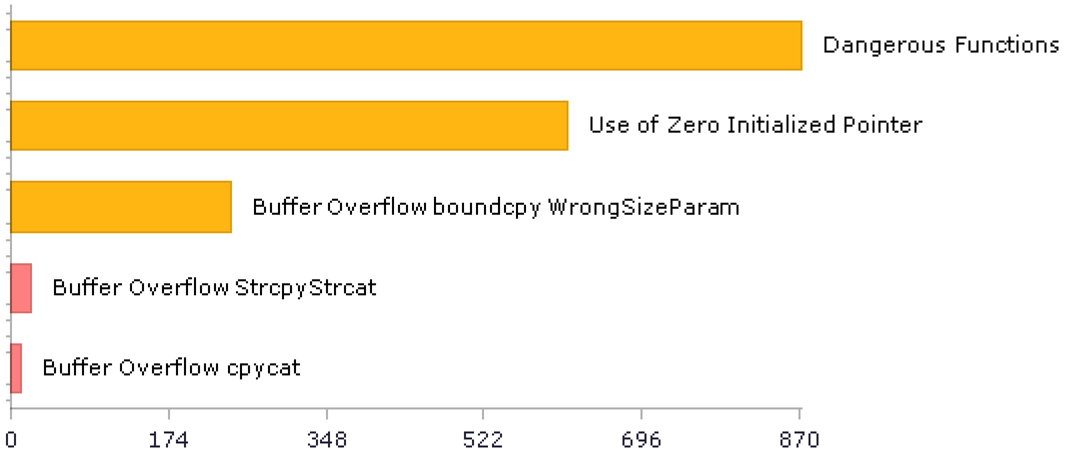
Result Summary



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	351	294
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
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	872	872
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control*	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities*	EXTERNAL USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	872	872
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	2	2
PCI DSS (3.2) - 6.5.2 - Buffer overflows	279	256
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.	0	0
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.	0	0
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.	0	0
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.	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 - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*****	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*****	662	78
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*****	119	98
SI-11 Error Handling (P2)*****	64	64
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	5	3

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

Scan Summary - 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

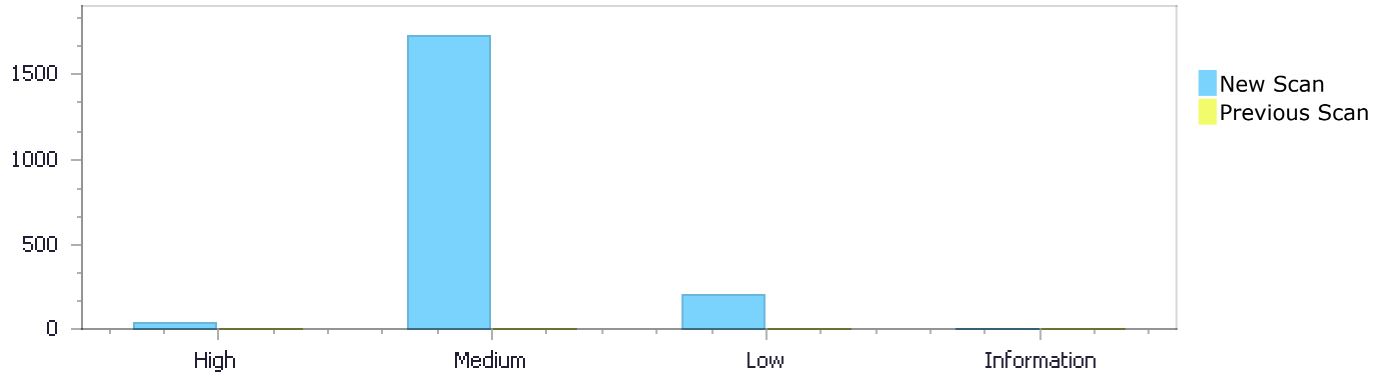
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	34	1,734	198	0	1,966
Recurrent Issues	0	0	0	0	0
Total	34	1,734	198	0	1,966

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	34	1,734	198	0	1,966
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	34	1,734	198	0	1,966

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	22	High
Buffer Overflow cpycat	12	High
Dangerous Functions	872	Medium
Use of Zero Initialized Pointer	614	Medium
Buffer Overflow boundcpy WrongSizeParam	242	Medium

Buffer Overflow Loops	3	Medium
Divide By Zero	2	Medium
Use of Uninitialized Variable	1	Medium
Unchecked Return Value	64	Low
Unchecked Array Index	62	Low
NULL Pointer Dereference	47	Low
Potential Precision Problem	23	Low
Potential Off by One Error in Loops	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	235
gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	235
gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	235
gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	118
gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	118
gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	118
gpac@@gpac-v0.9.0-preview-CVE-2024-6062-TP.c	118
gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	63
gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	63
gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	63

Scan Results Details

Buffer Overflow StrcpyStrcat

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

Categories

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

Description

Buffer Overflow StrcpyStrcat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=13
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.               strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=14
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                                sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.              strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=15
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method	void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                          sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.         strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=16
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method	void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                          sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.         strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=17
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                          sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.           strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=18
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.              strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=19
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.       strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=20
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.       strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=21
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c

Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                                sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.              strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=22
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c

Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                                sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.                 strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=23
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.         strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=24
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                          sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.        strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=25
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_text_get_utf8_line passes to szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	228	306
Object	szLine	szLine

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
228.  char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE
*txt_in, s32 unicode_type)
....
306.        strcpy(szLine, szLineConv);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=26
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_text_get_utf8_line passes to szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	228	306
Object	szLine	szLine

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
228.  char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE
*txt_in, s32 unicode_type)
....
306.        strcpy(szLine, szLineConv);
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=27
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_bt_peek_node passes to defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c

Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)

```
....
1578.  GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)
....
1600.       strcpy(nName, defID);
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=28
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_bt_peek_node passes to defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)

```
....
1578.  GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)
....
1600.       strcpy(nName, defID);
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=29
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_bt_peek_node passes to defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	1578	1600
Object	defID	defID

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)

```
....
1578.   GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)
....
1600.         strcpy(nName, defID);
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=30
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_bt_peek_node passes to defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)

```
....
1578.   GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)
....
1600.         strcpy(nName, defID);
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=31
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_bt_peek_node passes to defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)

```
....
1578.  GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)
....
1600.        strcpy(nName, defID);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=32
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_bt_peek_node passes to defID, at line 1578 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)

```
....
1578.  GF_Node *gf_bt_peek_node(GF_BTParser *parser, char *defID)
....
1600.        strcpy(nName, defID);
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=33
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_text_get_utf8_line passes to szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	228	306
Object	szLine	szLine

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
228.  char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE
*txt_in, s32 unicode_type)
....
306.        strcpy(szLine, szLineConv);
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=34
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2024-6062-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_text_get_utf8_line passes to szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2024-6062-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-6062-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-6062-TP.c
Line	228	306
Object	szLine	szLine

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2024-6062-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
228.  char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE
*txt_in, s32 unicode_type)
....
306.        strcpy(szLine, szLineConv);
```

Buffer Overflow cpycat

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow cpycat Version:0

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 cpycat\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                        sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.             strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=2
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                                sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▾

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.                 strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=3
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c

Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                         sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.       strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=4
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                         sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.        strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=5
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                         sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.            strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=6
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.             strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=7
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.        strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=8
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                        sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c

Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.        strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=9
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.             strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=10
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                              sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1950.                  strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=11
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                              sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.            strcpy(nstr, gf_bt_get_next(parser, 1));
```

Buffer Overflow cpycat\Path 12:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=12
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_bt_check_line passes to Address, at line 137 of gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	void gf_bt_check_line(GF_BTParser *parser)

```
....
377.                            sscanf(buf, "%dx%d", &parser->def_w,
&parser->def_h);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	GF_Route *gf_bt_parse_route(GF_BTParser *parser, Bool skip_def, Bool is_insert, GF_Command *com)

```
....
1983.       strcpy(nstr, gf_bt_get_next(parser, 1));
```

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=1000022&projectid=17&pathid=282
Status	New

The dangerous function, memcpy, was found in use at line 502 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	1993	1993
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
1993.             memcpy(udesc.compressor_name+1, comp_name, len);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=283
Status	New

The dangerous function, memcpy, was found in use at line 2550 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2574	2574
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2574.             memcpy(constant_IV, p->value.data.ptr,
constant_IV_size);
```

Dangerous Functions\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=284
Status	New

The dangerous function, memcpy, was found in use at line 2550 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2581	2581
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2581.             memcpy(KID, p->value.data.ptr, 16);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=285
Status	New

The dangerous function, memcpy, was found in use at line 2550 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2644	2644
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2644.             memcpy(tkw->KID, KID, sizeof(bin128));
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=286
Status	New

The dangerous function, memcpy, was found in use at line 2550 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2648	2648
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2648.              memcpy(tkw->constant_IV, constant_IV, sizeof(bin128));
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=287
Status	New

The dangerous function, memcpy, was found in use at line 4442 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4449	4449
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_on_data_patch(void *cbk, u8 *data, u32 block_size, u64 file_offset, Bool is_insert)

```
....
4449.        memcpy(output, data, block_size);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=288
Status	New

The dangerous function, memcpy, was found in use at line 4459 in gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4510	4510
Object	memcpy	memcpy

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_on_data(void *cbk, u8 *data, u32 block_size)

```
....
4510.            memcpy(output, data, block_size);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=289
Status	New

The dangerous function, memcpy, was found in use at line 421 in gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Line	465	465
Object	memcpy	memcpy

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c

Method GF_Err latm_dmx_process(GF_Filter *filter)

```
....
465.          memcpy(ctx->latm_buffer + ctx->latm_buffer_size, data,
pck_size);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=290
Status	New

The dangerous function, memcpy, was found in use at line 421 in gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Line	508	508
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

```
....
508.                memcpy(output, latm_buffer, latm_frame_size);
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=291
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	434	434
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method	GF_Err h263dmx_process(GF_Filter *filter)

```
....
434.                    memcpy(ctx->hdr_store, start, remain);
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=292
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	444	444
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method	GF_Err h263dmx_process(GF_Filter *filter)

```
....
444.                    memcpy(ctx->hdr_store + ctx->bytes_in_header,
start, 8 - ctx->bytes_in_header);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=293
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	452	452

Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
452.                          memcpy(pck_data, ctx->hdr_store, ctx-
>bytes_in_header);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=294
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	500	500
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
500.                          memcpy(pck_data, ctx->hdr_store, current);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=295
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c

Line	505	505
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
505.                                    memcpy(pck_data, start, current);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=296
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	561	561
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
561.                                    memcpy(ctx->hdr_store, start+remain-3, 3);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=297
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-	gpac@@gpac-v0.9.0-preview-CVE-2022-

	47663-TP.c	47663-TP.c
Line	572	572
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
572.                    memcpy(pck_data, ctx->hdr_store+current, ctx-
>bytes_in_header);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=298
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	578	578
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
578.                    memcpy(pck_data, start, size);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=299
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Line	580	580
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

```
....
580.                        memcpy(pck_data, start, size);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=300
Status	New

The dangerous function, memcpy, was found in use at line 930 in gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	952	952
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method static void gf_webvtt_flush_sample(void *user, GF_WebVTTSample *samp)

```
....
952.                memcpy(pck_data, s->data, s->dataLength);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=301
Status	New

The dangerous function, memcpy, was found in use at line 1270 in gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	1431	1431
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static GF_Err gf_text_process_ttml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1431.                              memcpy(pck_data, txt_str, txt_len);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=302
Status	New

The dangerous function, memcpy, was found in use at line 1468 in gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	1482	1482
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static GF_Err swf_svg_add_iso_sample(void *user, const u8 *data, u32 length, u64 timestamp, Bool isRap)

```
....
1482.        memcpy(pck_data, data, length);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=303
Status	New

The dangerous function, memcpy, was found in use at line 1494 in gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	1507	1507
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static GF_Err swf_svg_add_iso_header(void *user, const u8 *data, u32 length, Bool isHeader)

```
....
1507.               memcpy(pck_data, data, length);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=304
Status	New

The dangerous function, memcpy, was found in use at line 476 in gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Line	530	530
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Method	GF_Err adts_dmx_process(GF_Filter *filter)

```
....
530.                memcpy(ctx->adts_buffer + ctx->adts_buffer_size, data, 
pck_size);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17

	&pathid=305
Status	New

The dangerous function, memcpy, was found in use at line 476 in gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Line	649	649
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

```
....
649.                    memcpy(output, sync + offset, size);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=306
Status	New

The dangerous function, memcpy, was found in use at line 930 in gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	952	952
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static void gf_webvtt_flush_sample(void *user, GF_WebVTTSample *samp)

```
....
952.                memcpy(pck_data, s->data, s->dataLength);
```

Dangerous Functions\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=307
Status	New

The dangerous function, memcpy, was found in use at line 1270 in gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	1431	1431
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static GF_Err gf_text_process_ttml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1431.                         memcpy(pck_data, txt_str, txt_len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=308
Status	New

The dangerous function, memcpy, was found in use at line 1468 in gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	1482	1482
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static GF_Err swf_svg_add_iso_sample(void *user, const u8 *data, u32 length, u64 timestamp, Bool isRap)

```
....
1482.        memcpy(pck_data, data, length);
```

Dangerous Functions\Path 28:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=309
Status	New

The dangerous function, memcpy, was found in use at line 1494 in gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	1507	1507
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static GF_Err swf_svg_add_iso_header(void *user, const u8 *data, u32 length, Bool isHeader)

```
....
1507.           memcpy(pck_data, data, length);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=310
Status	New

The dangerous function, memcpy, was found in use at line 1315 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1387.           memcpy(sl->data, data, size);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=311
Status	New

The dangerous function, memcpy, was found in use at line 1315 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1397	1397
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1397.       memcpy(sl->data, data, size);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=312
Status	New

The dangerous function, memcpy, was found in use at line 1593 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1661	1661
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static s32 naludmx_parse_nal_hevc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

```
....
1661.                    memcpy(ctx->sei_buffer + ctx->sei_buffer_size +
ctx->nal_length, data, size);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=313
Status	New

The dangerous function, memcpy, was found in use at line 1593 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1722	1722
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static s32 naludmx_parse_nal_hevc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

```
....
1722.                    memcpy(ctx->init_aud, data, 3);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=314
Status	New

The dangerous function, memcpy, was found in use at line 1752 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1816	1816
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static s32 naludmx_parse_nal_avc(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 nal_type, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

```
....
1816.                   memcpy(ctx->sei_buffer + ctx->sei_buffer_size +
ctx->nal_length, data, sei_size);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=315
Status	New

The dangerous function, memcpy, was found in use at line 1752 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1840	1840
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static s32 naludmx_parse_nal_avc(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 nal_type, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

```
....
1840.                   memcpy(ctx->init_aud, data, 2);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=316
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Line	2021	2021
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

```
....
2021.            memcpy(ctx->hdr_store + ctx->hdr_store_size, data,
sizeof(char)*pck_size);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=317
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2101	2101
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

```
....
2101.                  memcpy(ctx->hdr_store, start, remain);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=318
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2112	2112
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2112.                   memcpy(ctx->hdr_store + ctx->bytes_in_header,
start, SAFETY_NAL_STORE - ctx->bytes_in_header);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=319
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2122	2122
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2122.                                     memcpy(pck_data, ctx-
>hdr_store, ctx->bytes_in_header);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=320
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2217	2217
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2217.                                       memcpy(pck_data, start, 
(size_t) size);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=321
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2221	2221
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2221.                                   memcpy(ctx->hdr_store, start+remain-
3, 3);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=322
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2264	2264
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2264.                               memcpy(pck_data, ctx->hdr_store,
current);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=323
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2268	2268
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2268.                               memcpy(pck_data, start, current);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=324

Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2369	2369
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2369.                                    memcpy(ctx->hdr_store + ctx-
>hdr_store_size, start, sizeof(char)*pck_avail);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=325
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2408	2408
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2408.                                                  memcpy(ctx->hdr_store +
hdr_offset + nal_bytes_from_store, start, copy_size);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=326
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2421	2421
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

```
....
2421.                               memcpy(ctx->hdr_store, start,
remain);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=327
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2468	2468
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

```
....
2468.                               memcpy(ctx->hdr_store, start+remain-
3, 3);
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=328
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2607	2607
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2607.                                   memcpy(ctx->svc_prefix_buffer,
start+sc_size, ctx->svc_prefix_buffer_size);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=329
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2805	2805
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2805.                    memcpy(pck_data + ctx->nal_length , ctx-
>init_aud, audelim_size);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=330
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2814	2814
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2814.                    memcpy(pck_data, ctx->sei_buffer, ctx-
>sei_buffer_size);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=331
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2823	2823
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

```
....
2823.                        memcpy(pck_data + ctx->nal_length, ctx-
>svc_prefix_buffer, ctx->svc_prefix_buffer_size);
```

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=1000022&projectid=17&pathid=1353
Status	New

The variable declared in keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2511 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2513	2537
Object	keyIDs	keyIDs

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2513.        bin128 *keyIDs=NULL;
....
2537.                        keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1354
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3330 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3582	2537
Object	dst_pck	keyIDs

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.             ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2537.                   keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1355
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3303	2537
Object	dst_pck	keyIDs

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.             ctx->dst_pck = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2537.                       keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1356
Status	New

The variable declared in avc_state at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 309 is not initialized when it is used by avc_state at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 309.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	314	412
Object	avc_state	avc_state

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

```
....
314.            AVCState *avc_state = NULL;
....
412.                        nal_type = avc_state->last_nal_type_parsed;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1357
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	558	567

Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
558.                pa = NULL;
....
567.          gf_list_add(pa->nalus, sl);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1358
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	552	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.          GF_HEVCParamArray *pa = NULL;
....
567.          gf_list_add(pa->nalus, sl);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1359
Status	New

The variable declared in buf at gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c in line 207 is not initialized when it is used by buf at gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c in line 207.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Line	210	244
Object	buf	buf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Method static void mp3_dmx_flush_id3(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
210.        char *buf=NULL;
....
244.                    buf = gf_realloc(buf, fsize+2);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1360
Status	New

The variable declared in offset_table at gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c in line 1416 is not initialized when it is used by offset_table at gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c in line 1416.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1421	1487
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1421.       u32 *offset_table = NULL;
....
1487.                           e = swf_seek_file_to(read, start + 
offset_table[i]);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1361
Status	New

The variable declared in st at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by st at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	270
Object	st	st

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                                    st = NULL;
....
270.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_STREAM_TYPE, &PROP_UINT(GF_STREAM_AUDIO) );
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1362
Status	New

The variable declared in st at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by st at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	270
Object	st	st

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                            AVIAstream *st = NULL;
....
270.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_STREAM_TYPE, &PROP_UINT(GF_STREAM_AUDIO) );
```

Use of Zero Initialized Pointer\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1363
Status	New

The variable declared in offset_table at gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c in line 1416 is not initialized when it is used by offset_table at gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c in line 1416.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1421	1487
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1421.       u32 *offset_table = NULL;
....
1487.                          e = swf_seek_file_to(read, start + 
offset_table[i]);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1364
Status	New

The variable declared in keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c in line 2511 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	2513	2537
Object	keyIDs	keyIDs

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2513.       bin128 *keyIDs=NULL;
....
2537.                   keyIDs = gf_realloc(keyIDs, 
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1365
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c in line 3330 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	3582	2537
Object	dst_pck	keyIDs

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c

Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.               ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c

Method static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2537.                         keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1366
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c in line 3285 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	3303	2537
Object	dst_pck	keyIDs

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.               ctx->dst_pck = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2537.                       keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1367
Status	New

The variable declared in offset_table at gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c in line 1416 is not initialized when it is used by offset_table at gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c in line 1416.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1421	1487
Object	offset_table	offset_table

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1421.       u32 *offset_table = NULL;
....
1487.                             e = swf_seek_file_to(read, start +
offset_table[i]);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1368
Status	New

The variable declared in keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c in line 2511 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	2513	2537
Object	keyIDs	keyIDs

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2513.       bin128 *keyIDs=NULL;
....
2537.                   keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1369
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c in line 3330 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	3582	2537
Object	dst_pck	keyIDs

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.           ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2537.                    keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1370
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c in line 3285 is not initialized when it is used by keyIDs at gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c in line 2511.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	3303	2537
Object	dst_pck	keyIDs

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c

Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.             ctx->dst_pck = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c

Method static void mp4_mux_cenc_insert_pssh(GF_MP4MuxCtx *ctx, TrackWriter *tkw)

```
....
2537.                    keyIDs = gf_realloc(keyIDs,
sizeof(bin128)*max_keys);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1371
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3330 is not initialized when it is used by tkw at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3582	3308
Object	dst_pck	tkw

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.           ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3308.           tkw = gf_list_get(ctx->tracks, 0);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1372
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285 is not initialized when it is used by tkw at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3303	3308
Object	dst_pck	tkw

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.           ctx->dst_pck = NULL;
....
3308.           tkw = gf_list_get(ctx->tracks, 0);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1373
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3330 is not initialized when it is used by seg_sizes at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3774.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3582	4079
Object	dst_pck	seg_sizes

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.              ctx->dst_pck = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_fragmented(GF_Filter *filter, GF_MP4MuxCtx *ctx)

```
....
4079.                                 ctx->seg_sizes = gf_realloc(ctx-
>seg_sizes, sizeof(u32) * ctx->alloc_seg_sizes);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1374
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285 is not initialized when it is used by seg_sizes at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3774.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3303	4079
Object	dst_pck	seg_sizes

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.                ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_fragmented(GF_Filter *filter, GF_MP4MuxCtx *ctx)

```
....
4079.                              ctx->seg_sizes = gf_realloc(ctx-
>seg_sizes, sizeof(u32) * ctx->alloc_seg_sizes);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1375
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3330 is not initialized when it is used by au_delim at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2728.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3582	2882
Object	dst_pck	au_delim

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.                ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_sample(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, Bool for_fragment)

```
....
2882.                                  au_delim = pck_data;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1376
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285 is not initialized when it is used by au_delim at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2728.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3303	2882
Object	dst_pck	au_delim

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.               ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_sample(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, Bool for_fragment)

```
....
2882.                                   au_delim = pck_data;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1377
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3330 is not initialized when it is used by au_delim at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2728.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3582	2888
Object	dst_pck	au_delim

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.               ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_sample(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, Bool for_fragment)

```
....
2888.                                 au_delim = pck_data;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1378
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285 is not initialized when it is used by au_delim at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2728.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3303	2888
Object	dst_pck	au_delim

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.               ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_sample(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, Bool for_fragment)

```
....
2888.                                 au_delim = pck_data;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1379
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3330 is not initialized when it is used by subs at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2728.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3582	2744
Object	dst_pck	subs

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_initialize_movie(GF_MP4MuxCtx *ctx)

```
....
3582.                  ctx->dst_pck = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method static GF_Err mp4_mux_process_sample(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, Bool for_fragment)

```
....
2744.           subs = gf_filter_pck_get_property(pck, GF_PROP_PCK_SUBS);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1380
Status	New

The variable declared in dst_pck at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 3285 is not initialized when it is used by subs at gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c in line 2728.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3303	2744
Object	dst_pck	subs

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static void mp4_mux_flush_frag(GF_MP4MuxCtx *ctx, Bool is_init, u64 idx_start_range, u64 idx_end_range)

```
....
3303.               ctx->dst_pck = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_process_sample(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, Bool for_fragment)

```
....
2744.        subs = gf_filter_pck_get_property(pck, GF_PROP_PCK_SUBS);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1381
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 936 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1064	1329
Object	Pointer	list

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	void naludmx_create_avc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar)

```
....
1064.        *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1329.                    list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1382
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 770 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	902	1329
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_create_hevc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar, Bool *has_hevc_base)

```
....
902.        *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1329.                   list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1383
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1501 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Line	1507	1329
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1507.         *data_ptr = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1329.                       list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1384
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 770 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	902	1342
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_create_hevc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar, Bool *has_hevc_base)

```
....
902.          *dsi = *dsi_enh = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1342.                        list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1385
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 936 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1064	1342
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method void naludmx_create_avc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar)

```
....
1064.        *dsi = *dsi_enh = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1342.                        list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1386
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1501 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1507	1342
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1507.        *data_ptr = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1342.                    list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1387
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 936 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1064	1326
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method void naludmx_create_avc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar)

```
....
1064.        *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1326.                    list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1388
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 770 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	902	1326
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_create_hevc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar, Bool *has_hevc_base)

```
....
902.         *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1326.                    list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1389

Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1501 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1507	1326
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1507.         *data_ptr = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1326.                         list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1390
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1501 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1533.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1507	1544
Object	Pointer	first_pck_in_au

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1507.        *data_ptr = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method GF_FilterPacket *naludmx_start_nalu(GF_NALUDmxCtx *ctx, u32 nal_size, Bool skip_nal_field, Bool *au_start, u8 **pck_data)

```
....
1544.              ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1391
Status	New

The variable declared in first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1406 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1533.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1487	1544
Object	first_pck_in_au	first_pck_in_au

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method void naludmx_finalize_au_flags(GF_NALUDmxCtx *ctx)

```
....
1487.        ctx->first_pck_in_au = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method GF_FilterPacket *naludmx_start_nalu(GF_NALUDmxCtx *ctx, u32 nal_size, Bool skip_nal_field, Bool *au_start, u8 **pck_data)

```
....
1544.              ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 40:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1392
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 770 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1533.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	902	1544
Object	Pointer	first_pck_in_au

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_create_hevc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar, Bool *has_hevc_base)

```
....
902.         *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_FilterPacket *naludmx_start_nalu(GF_NALUDmxCtx *ctx, u32 nal_size, Bool skip_nal_field, Bool *au_start, u8 **pck_data)

```
....
1544.              ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1393
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 936 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1533.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1064	1544
Object	Pointer	first_pck_in_au

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method void naludmx_create_avc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar)

```
....
1064.        *dsi = *dsi_enh = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method GF_FilterPacket *naludmx_start_nalu(GF_NALUDmxCtx *ctx, u32 nal_size, Bool skip_nal_field, Bool *au_start, u8 **pck_data)

```
....
1544.              ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1394
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 770 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	902	1332
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_create_hevc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar, Bool *has_hevc_base)

```
....
902.         *dsi = *dsi_enh = NULL;
```

▼

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1332.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1395
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 936 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1064	1332
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method void naludmx_create_avc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar)

```
....
1064.        *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1332.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1396
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1501 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1507	1332
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1507.        *data_ptr = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1332.                        list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1397
Status	New

The variable declared in first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1406 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1487	1332
Object	first_pck_in_au	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method void naludmx_finalize_au_flags(GF_NALUDmxCtx *ctx)

```
....
1487.        ctx->first_pck_in_au = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1332.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1398
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 770 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	902	1345
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_create_hevc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar, Bool *has_hevc_base)

```
....
902.         *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1345.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1399
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 936 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1064	1345
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method void naludmx_create_avc_decoder_config(GF_NALUDmxCtx *ctx, u8 **dsi, u32 *dsi_size, u8 **dsi_enh, u32 *dsi_enh_size, u32 *max_width, u32 *max_height, u32 *max_enh_width, u32 *max_enh_height, GF_Fraction *sar)

```
....
1064.        *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1345.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1400
Status	New

The variable declared in Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1501 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1507	1345
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1507.        *data_ptr = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1345.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1401
Status	New

The variable declared in first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1406 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1487	1345
Object	first_pck_in_au	list

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method void naludmx_finalize_au_flags(GF_NALUDmxCtx *ctx)

```
....
1487.        ctx->first_pck_in_au = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1345.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17

	&pathid=1402
Status	New

The variable declared in first_pck_in_au at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1406 is not initialized when it is used by list at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 1315.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	1487	1350
Object	first_pck_in_au	list

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method void naludmx_finalize_au_flags(GF_NALUDmxCtx *ctx)

```
....
1487.        ctx->first_pck_in_au = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c

Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

```
....
1350.                  list = ctx->sps_ext;
```

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=1000022&projectid=17&pathid=37
Status	New

The size of the buffer used by mp4_mux_cenc_update in bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_cenc_update passes to bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-	gpac@@gpac-v0.9.0-preview-CVE-2022-

	47654-TP.c	47654-TP.c
Line	2644	2644
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2644.             memcpy(tkw->KID, KID, sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=38
Status	New

The size of the buffer used by mp4_mux_cenc_update in bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_cenc_update passes to bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2648	2648
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2648.             memcpy(tkw->constant_IV, constant_IV, sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=39
Status	New

The size of the buffer used by BD_XReplace in GF_FieldInfo, at line 49 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BD_XReplace passes to GF_FieldInfo, at line 49 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	180	180
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Method	static GF_Err BD_XReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
180.                            memcpy(&sffield, &targetField,
sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=40
Status	New

The size of the buffer used by BD_DecMultipleIndexReplace in GF_FieldInfo, at line 285 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BD_DecMultipleIndexReplace passes to GF_FieldInfo, at line 285 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	325	325
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Method	static GF_Err BD_DecMultipleIndexReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
325.         memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=41

Status	New

The size of the buffer used by BD_DecIndexInsert in GF_FieldInfo, at line 581 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BD_DecIndexInsert passes to GF_FieldInfo, at line 581 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	620	620
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c

Method static GF_Err BD_DecIndexInsert(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
620.        memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=42
Status	New

The size of the buffer used by BD_DecIndexValueReplace in GF_FieldInfo, at line 827 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BD_DecIndexValueReplace passes to GF_FieldInfo, at line 827 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	883	883
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c

Method static GF_Err BD_DecIndexValueReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
883.            memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=43
Status	New

The size of the buffer used by BM_ParseIndexInsert in GF_FieldInfo, at line 444 of gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BM_ParseIndexInsert passes to GF_FieldInfo, at line 444 of gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c
Line	485	485
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c
Method	GF_Err BM_ParseIndexInsert(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
485.        memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=44
Status	New

The size of the buffer used by BM_ParseIndexValueReplace in GF_FieldInfo, at line 732 of gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BM_ParseIndexValueReplace passes to GF_FieldInfo, at line 732 of gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c
Line	783	783
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c
Method	GF_Err BM_ParseIndexValueReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
783.              memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=45
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *swf_clone_shape_rec passes to SWFShapeRec, at line 360 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
363.         memcpy(new_sr, old_sr, sizeof(SWFShapeRec));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=46
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1362	1362
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1362.                         memcpy(&mat, &ds->mat,
sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=47
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1366	1366
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1366.                         memcpy(&cmat, &ds->cmat,
sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=48
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1385	1385
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1385.        memcpy(&ds->mat, &mat, sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=49
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1386	1386
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1386.        memcpy(&ds->cmat, &cmat, sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=50
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *swf_clone_shape_rec passes to SWFShapeRec, at line 360 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
363.        memcpy(new_sr, old_sr, sizeof(SWFShapeRec));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=51
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1362	1362
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1362.                       memcpy(&mat, &ds->mat,
sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=52
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c

Line	1366	1366
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1366.                           memcpy(&cmat, &ds->cmat, 
sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=53
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1385	1385
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1385.         memcpy(&ds->mat, &mat, sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=54
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1386	1386
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1386.        memcpy(&ds->cmat, &cmat, sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=55
Status	New

The size of the buffer used by mp4_mux_cenc_update in bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_cenc_update passes to bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	2644	2644
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2644.               memcpy(tkw->KID, KID, sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=56
Status	New

The size of the buffer used by mp4_mux_cenc_update in bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_cenc_update passes to bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	2648	2648
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2648.           memcpy(tkw->constant_IV, constant_IV, sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=57
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *swf_clone_shape_rec passes to SWFShapeRec, at line 360 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
363.        memcpy(new_sr, old_sr, sizeof(SWFShapeRec));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=58
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1362	1362
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1362.                        memcpy(&mat, &ds->mat,
sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=59
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1366	1366
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1366.                        memcpy(&cmat, &ds->cmat,
sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17

	&pathid=60
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_Matrix2D, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1385	1385
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1385.       memcpy(&ds->mat, &mat, sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=61
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_place_obj passes to GF_ColorMatrix, at line 1245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1386	1386
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1386.       memcpy(&ds->cmat, &cmat, sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=62
Status	New

The size of the buffer used by mp4_mux_cenc_update in bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_cenc_update passes to bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	2644	2644
Object	bin128	bin128

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method	static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2644.            memcpy(tkw->KID, KID, sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=63
Status	New

The size of the buffer used by mp4_mux_cenc_update in bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_cenc_update passes to bin128, at line 2550 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	2648	2648
Object	bin128	bin128

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method	static GF_Err mp4_mux_cenc_update(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck, u32 act_type, u32 pck_size)

```
....
2648.            memcpy(tkw->constant_IV, constant_IV, sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=64
Status	New

The size of the buffer used by isor_reader_get_sample in bin128, at line 200 of gpac@@gpac-v0.9.0-preview-CVE-2023-48013-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that isor_reader_get_sample passes to bin128, at line 200 of gpac@@gpac-v0.9.0-preview-CVE-2023-48013-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-48013-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-48013-TP.c
Line	483	483
Object	bin128	bin128

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-48013-TP.c
Method	void isor_reader_get_sample(ISOMChannel *ch)

```
....
483.                        memcpy(ch->KID, KID,
sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=65
Status	New

The size of the buffer used by mp4_mux_setup_pid in GF_3GPConfig, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_setup_pid passes to GF_3GPConfig, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	1807	1807
Object	GF_3GPConfig	GF_3GPConfig

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
1807.                memset(&gpp_cfg, 0, sizeof(GF_3GPConfig));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=66
Status	New

The size of the buffer used by mp4_mux_setup_pid in GF_AC3Config, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_setup_pid passes to GF_AC3Config, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	1845	1845
Object	GF_AC3Config	GF_AC3Config

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
1845.                memset(&ac3cfg, 0, sizeof(GF_AC3Config));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=67
Status	New

The size of the buffer used by mp4_mux_setup_pid in GF_GenericSampleDescription, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_setup_pid passes to GF_GenericSampleDescription, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	1987	1987
Object	GF_GenericSampleDescription	GF_GenericSampleDescription

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
1987.               memset(&udesc, 0,
sizeof(GF_GenericSampleDescription));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=68
Status	New

The size of the buffer used by mp4_mux_setup_pid in GF_AudioChannelLayout, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_setup_pid passes to GF_AudioChannelLayout, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2257	2257
Object	GF_AudioChannelLayout	GF_AudioChannelLayout

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
2257.                       memset(&layout, 0,
sizeof(GF_AudioChannelLayout));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=69
Status	New

The size of the buffer used by mp4_mux_setup_pid in AVCState, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_setup_pid passes to AVCState, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	2367	2367
Object	AVCState	AVCState

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
2367.                 memset(&avc, 0, sizeof(AVCState));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=70
Status	New

The size of the buffer used by mp4_mux_process_item in GF_ImageItemProperties, at line 3090 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_process_item passes to GF_ImageItemProperties, at line 3090 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	3143	3143
Object	GF_ImageItemProperties	GF_ImageItemProperties

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method static GF_Err mp4_mux_process_item(GF_MP4MuxCtx *ctx, TrackWriter *tkw, GF_FilterPacket *pck)

```
....
3143.        memset(&image_props, 0, sizeof(GF_ImageItemProperties));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=71
Status	New

The size of the buffer used by latm_dmx_check_dur in GF_M4ADecSpecInfo, at line 215 of gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that latm_dmx_check_dur passes to GF_M4ADecSpecInfo, at line 215 of gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Line	243	243
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Method static void latm_dmx_check_dur(GF_Filter *filter, GF_LATMDmxCtx *ctx)

```
....
243.        memset(&acfg, 0, sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=72
Status	New

The size of the buffer used by ttxt_parse_text_box in GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_box passes to GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	1755	1755
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method static void ttxt_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
1755.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=73

Status	New

The size of the buffer used by ttxt_parse_text_style in GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_style passes to GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	1768	1768
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method static void ttxt_parse_text_style(GF_TXTIn *ctx, GF_XMLNode *n, GF_StyleRecord *style)

```
....
1768.        memset(style, 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=74
Status	New

The size of the buffer used by txtin_setup_ttxt in GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_setup_ttxt passes to GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	1873	1873
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method static GF_Err txtin_setup_ttxt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1873.                              memset(&td, 0, 
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=75
Status	New

The size of the buffer used by tx3g_parse_text_box in GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tx3g_parse_text_box passes to GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	2199	2199
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static void tx3g_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
2199.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=76
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	2351	2351
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2351.                           memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=77
Status	New

The size of the buffer used by txtin_process_texml in GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	2418	2418
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2418.
        memset(&styles[nb_styles], 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=78
Status	New

The size of the buffer used by txtin_process_texml in Marker, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to Marker, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	2535	2535
Object	Marker	Marker

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method	static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2535.
        memset(&marks[nb_marks], 0, sizeof(Marker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=79
Status	New

The size of the buffer used by adts_dmx_check_pid in GF_M4ADecSpecInfo, at line 253 of gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that adts_dmx_check_pid passes to GF_M4ADecSpecInfo, at line 253 of gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Line	325	325
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Method	static void adts_dmx_check_pid(GF_Filter *filter, GF_ADTSDmxCtx *ctx)

```
....
325.            memset(&acfg, 0, sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=80
Status	New

The size of the buffer used by *adts_dmx_probe_data in ADTSHeader, at line 713 of gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *adts_dmx_probe_data passes to ADTSHeader, at line 713 of gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Line	718	718
Object	ADTSHeader	ADTSHeader

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-0866-TP.c
Method	static const char *adts_dmx_probe_data(const u8 *data, u32 size, GF_FilterProbeScore *score)

```
....
718.        memset(&prev_hdr, 0, sizeof(ADTSHeader));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=81
Status	New

The size of the buffer used by ttxt_parse_text_box in GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_box passes to GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	1755	1755
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method	static void ttxt_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
1755.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=82
Status	New

The size of the buffer used by ttxt_parse_text_style in GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_style passes to GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	1768	1768

Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static void ttxt_parse_text_style(GF_TXTIn *ctx, GF_XMLNode *n, GF_StyleRecord *style)

```
....
1768.       memset(style, 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=83
Status	New

The size of the buffer used by txtin_setup_ttxt in GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_setup_ttxt passes to GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	1873	1873
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static GF_Err txtin_setup_ttxt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1873.                       memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=84
Status	New

The size of the buffer used by tx3g_parse_text_box in GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tx3g_parse_text_box passes to GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	2199	2199
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static void tx3g_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
2199.        memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=85
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	2351	2351
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2351.                          memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=86
Status	New

The size of the buffer used by txtin_process_texml in GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	2418	2418
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2418.
        memset(&styles[nb_styles], 0, sizeof(GF_StyleRecord));
```

Buffer Overflow Loops

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

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow Loops\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=279
Status	New

The buffer allocated by c in gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c at line 254 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c
Line	313	330
Object	16	c

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c
Method GF_Err vobsub_read_idx(FILE *file, vobsub_file *vobsub, s32 *version)

```
....
313.                    u8  palette[16][4];
....
330.                          g = palette[c][1];
```

Buffer Overflow Loops\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=280
Status	New

The buffer allocated by c in gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c at line 254 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c
Line	313	329
Object	16	c

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c
Method	GF_Err vobsub_read_idx(FILE *file, vobsub_file *vobsub, s32 *version)

```
....
313.                    u8  palette[16][4];
....
329.                          r = palette[c][2];
```

Buffer Overflow Loops\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=281
Status	New

The buffer allocated by c in gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c at line 254 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c
Line	313	331
Object	16	c

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-3523-TP.c
Method	GF_Err vobsub_read_idx(FILE *file, vobsub_file *vobsub, s32 *version)

```
....
313.                    u8  palette[16][4];
....
331.                           b = palette[c][0];
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=35
Status	New

The application performs an illegal operation in mp3_dmx_check_dur, in gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c. In line 111, the program attempts to divide by prev_sr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input prev_sr in mp3_dmx_check_dur of gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c, at line 111.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Line	148	148
Object	prev_sr	prev_sr

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Method	static void mp3_dmx_check_dur(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
148.                    duration /= prev_sr;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=36
Status	New

The application performs an illegal operation in mp3_dmx_check_dur, in gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c. In line 111, the program attempts to divide by prev_sr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input prev_sr in mp3_dmx_check_dur of gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c, at line 111.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Line	151	151
Object	prev_sr	prev_sr

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Method static void mp3_dmx_check_dur(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
151.                    cur_dur /= prev_sr;
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Use of Uninitialized Variable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1352
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	534	553
Object	continuous	continuous

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method GF_Err avidmx_process(GF_Filter *filter)

```
....
534.                    int continuous;
....
553.                    if (continuous)
```

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=1000022&projectid=17&pathid=1154
Status	New

The mp4_mux_setup_pid method calls the snprintf function, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	951	951
Object	snprintf	snprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
951.                                   snprintf(szHName, 1024,
"*%s@GPAC%s", f ? f : "", gf_gpac_version() );
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1155
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4258	4258
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4258.            sprintf(szStatus, "waiting for clock init");
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1156
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4273	4273
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4273.                 sprintf(szStatus, "mux %d%%", pc);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1157
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4283	4283
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4283.                           sprintf(szStatus, "mux segments %d (frags
%d) next %02.02g", ctx->nb_segs, ctx->nb_frags_in_seg, ctx-
>next_frag_start);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1158
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4285	4285
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4285.                           sprintf(szStatus, "mux frags %d next
%02.02g", ctx->nb_frags, ctx->next_frag_start);
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1159
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4288	4288
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4288.                        sprintf(szStatus, "%s", ((ctx-
>store==MP4MX_MODE_FLAT) || (ctx->store==MP4MX_MODE_FASTSTART)) ? "mux"
: "import");
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1160
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4325	4325
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4325.                             sprintf(szTK, " TK%d(%c): %d", tkw-
>track_id, tkw->status_type, tkw->samples_in_frag);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1161
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4329	4329
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4329.                          sprintf(szTK, " %d %%", pc);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1162
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-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	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4333	4333
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4333.                          sprintf(szTK, " %s%d(%c): %d %%", tkw-
>is_item ? "IT" : "TK", tkw->track_id, tkw->status_type, pc/100);
```

Unchecked Return Value\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1163
Status	New

The naludmx_process method calls the sprintf function, at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2023-2839-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	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2890	2890
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx->height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1164
Status	New

The mp3_dmx_flush_id3 method calls the sprintf function, at line 207 of gpac@@gpac-v0.9.0-preview-CVE-2023-3291-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	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Line	315	315
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Method	static void mp3_dmx_flush_id3(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
315.                    sprintf(szTag, "tag:%s", gf_4cc_to_str(ftag));
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1165
Status	New

The gf_bifs_dec_proto_list method calls the sprintf function, at line 994 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-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	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	1027	1027
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Method	GF_Err gf_bifs_dec_proto_list(GF_BifsDecoder * codec, GF_BitStream *bs, GF_List *proto_list)

```
....
1027.                   sprintf(name, "Proto%d", gf_list_count(codec-
>current_graph->protos) );
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1166
Status	New

The gf_bifs_dec_proto_list method calls the sprintf function, at line 994 of gpac@@gpac-v0.9.0-preview-CVE-2023-37767-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	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	1051	1051
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Method	GF_Err gf_bifs_dec_proto_list(GF_BifsDecoder * codec, GF_BitStream *bs, GF_List *proto_list)

```
....
1051.                               sprintf(name, "_field%d", numFields);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1167
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2660	2660
Object	sprintf	sprintf

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2660.                               sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1168
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2662	2662
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2662.                         sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1169
Status	New

The swf_def_sound method calls the sprintf function, at line 1788 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1818	1818
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_def_sound(SWFReader *read)

```
....
1818.               sprintf(szName, "swf_sound_%d.mp3", snd->ID);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1170
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1960	1960
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.                    sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1171
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1962	1962
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                    sprintf(szName, "swf_soundstream_%d.mp3", read-
>current_sprite_id);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1172
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Line	2073	2073
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2073.           sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1173
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2075	2075
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2075.           sprintf(szName, "swf_jpeg_%d.jpg", ID);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1174
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2149	2149
Object	sprintf	sprintf

Code Snippet
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2149.                   sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1175
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-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	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2151	2151
Object	sprintf	sprintf

Code Snippet
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2151.                   sprintf(szName, "swf_png_%d.png", ID);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1176
Status	New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_sffield(GF_BTParser *parser, GF_FieldInfo *info, GF_Node *n)

```
....
951.                                    sprintf(szURL, "%u", id);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1177
Status	New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v0.9.0-preview-CVE-2023-4683-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Err gf_bt_parse_proto(GF_BTParser *parser, char *proto_code, GF_List *proto_list)

```
....
1858.                                   sprintf(szURL, "%d", url->OD_ID);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1178
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2660	2660
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2660.                            sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1179
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2662	2662
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2662.                            sprintf(svgFileName, "%s.svg", load->svgOutFile);
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17

	&pathid=1180
Status	New

The swf_def_sound method calls the sprintf function, at line 1788 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1818	1818
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_def_sound(SWFReader *read)

```
....
1818.             sprintf(szName, "swf_sound_%d.mp3", snd->ID);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1181
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1960	1960
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.                   sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1182
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1962	1962
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.               sprintf(szName, "swf_soundstream_%d.mp3", read->current_sprite_id);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1183
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2073	2073
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2073.            sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath, ID);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1184
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2075	2075
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2075.                sprintf(szName, "swf_jpeg_%d.jpg", ID);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1185
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2149	2149
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2149.                sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1186
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2151	2151
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2151.                sprintf(szName, "swf_png_%d.png", ID);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1187
Status	New

The mp4_mux_setup_pid method calls the snprintf function, at line 502 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	951	951
Object	snprintf	snprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	static GF_Err mp4_mux_setup_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_true_pid)

```
....
951.                            snprintf(szHName, 1024,
"*%s@GPAC%s", f ? f : "", gf_gpac_version() );
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1188
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4258	4258
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4258.             sprintf(szStatus, "waiting for clock init");
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1189
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4273	4273

Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4273.                   sprintf(szStatus, "mux %d%%", pc);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1190
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4283	4283
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4283.                         sprintf(szStatus, "mux segments %d (frags
%d) next %02.02g", ctx->nb_segs, ctx->nb_frags_in_seg, ctx-
>next_frag_start);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1191
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4285	4285
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4285.                              sprintf(szStatus, "mux frags %d next 
%02.02g", ctx->nb_frags, ctx->next_frag_start);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1192
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4288	4288
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4288.                        sprintf(szStatus, "%s", ((ctx-
>store==MP4MX_MODE_FLAT) || (ctx->store==MP4MX_MODE_FASTSTART)) ? "mux"
: "import");
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1193

Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4325	4325
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4325.                              sprintf(szTK, " TK%d(%c): %d", tkw-
>track_id, tkw->status_type, tkw->samples_in_frag);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1194
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4329	4329
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4329.                                    sprintf(szTK, " %d %%", pc);
```

Unchecked Return Value\Path 42:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1195
Status	New

The mp4_mux_format_report method calls the sprintf function, at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4333	4333
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4333.                           sprintf(szTK, " %s%d(%c): %d %%", tkw-
>is_item ? "IT" : "TK", tkw->track_id, tkw->status_type, pc/100);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1196
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2660	2660
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2660.                            sprintf(svgFileName, "%s%c%s.svg", load-
>localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1197
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2662	2662
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2662.                            sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1198
Status	New

The swf_def_sound method calls the sprintf function, at line 1788 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1818	1818
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static GF_Err swf_def_sound(SWFReader *read)

```
....
1818.                sprintf(szName, "swf_sound_%d.mp3", snd->ID);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1199
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1960	1960
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.                     sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1200
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1962	1962

Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                 sprintf(szName, "swf_soundstream_%d.mp3", read->current_sprite_id);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1201
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2073	2073
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2073.             sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath, ID);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1202
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-	gpac@@gpac-v0.9.0-preview-CVE-2023-

	4754-TP.c	4754-TP.c
Line	2075	2075
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2075.            sprintf(szName, "swf_jpeg_%d.jpg", ID);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1203
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-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	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2149	2149
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2149.                 sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

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=1000022&projectid=17

	&pathid=1290
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	245	245
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
245.                                szLineConv[j] = 0xc0 | ( (szLine[i]
>> 6) & 0x3 );
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1291
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	251	251
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
251.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1292
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	257	257
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
257.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1293
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	260	260
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
260.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1294
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c

Line	266	266
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
266.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1295
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	269	269
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
269.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1296
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	272	272
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
272.                                     szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1297
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	280	280
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
280.                          szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1298
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	283	283
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
283.                szLineConv[j] = 0;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1299
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Line	732	732
Object	alen	alen

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-0818-TP.c
Method static GF_Err txtin_process_srt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
732.                                    szLine[alen] = 0;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1300
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	245	245
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
245.                                    szLineConv[j] = 0xc0 | ( (szLine[i]
>> 6) & 0x3 );
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1301
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	251	251
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
251.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1302
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	257	257
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
257.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17

	&pathid=1303
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	260	260
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
260.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1304
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	266	266
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
266.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1305
Status	New

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	269	269
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
269.                                     szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1306
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	272	272
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
272.                                     szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1307
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	280	280

Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
280.                      szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1308
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	283	283
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
283.                szLineConv[j] = 0;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1309
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c
Line	732	732
Object	alen	alen

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-1452-TP.c

Method	static GF_Err txtin_process_srt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
732.                                    szLine[alen] = 0;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1310
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-23144-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-23144-TP.c
Line	307	307
Object	orient	orient

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-23144-TP.c
Method	GF_Err Q_DecCoordOnUnitSphere(GF_BifsDecoder *codec, GF_BitStream *bs, u32 NbBits, u32 NbComp, Fixed *m_ft)

```
....
307.             m_ft[orient] = delta;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1311
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	712	712
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
712.                                dep->dependent_on_layerID[dep->num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1312
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c
Line	212	212
Object	count	count

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c

Method static GF_Err BM_ParseProtoDelete(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
212.                    com->del_proto_list[count] = gf_bs_read_int(bs, 
codec->info->config.ProtoIDBits);
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1313
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-42298-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-42298-TP.c
Line	307	307
Object	orient	orient

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-42298-TP.c

Method GF_Err Q_DecCoordOnUnitSphere(GF_BifsDecoder *codec, GF_BitStream *bs, u32 NbBits, u32 NbComp, Fixed *m_ft)

```
....
307.        m_ft[orient] = delta;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1314
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Method static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
498.         sr->path->types[sr->path->nbType] = type;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1315
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Method static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
502.                sr->path->pts[sr->path->nbPts] = ctr;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1316
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
509.            sr->path->pts[sr->path->nbPts] = pt;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1317
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
509.            sr->path->pts[sr->path->nbPts] = pt;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1318
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Line	536	536
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method static void swf_referse_path(SWFPath *path)

```
....
536.                types[j] = path->types[path->nbType - i - 1];
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1319
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	3209	3209
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3209.                       odR->OD_ID[odR->NbODs] = id;
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1320
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c

Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
498.         sr->path->types[sr->path->nbType] = type;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1321
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
502.                 sr->path->pts[sr->path->nbPts] = ctr;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1322
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
509.                  sr->path->pts[sr->path->nbPts] = pt;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1323
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
509.                  sr->path->pts[sr->path->nbPts] = pt;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1324
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	536	536
Object	j	j

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method	static void swf_referse_path(SWFPath *path)

```
....
536.                  types[j] = path->types[path->nbType - i - 1];
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1325
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
498.        sr->path->types[sr->path->nbType] = type;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1326
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
502.                sr->path->pts[sr->path->nbPts] = ctr;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1327

Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
509.            sr->path->pts[sr->path->nbPts] = pt;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1328
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static void swf_path_add_com(SWFShapeRec *sr, SFVec2f pt, SFVec2f ctr, u32 type)

```
....
509.            sr->path->pts[sr->path->nbPts] = pt;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1329
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-	gpac@@gpac-v0.9.0-preview-CVE-2023-

	4754-TP.c	4754-TP.c
Line	536	536
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static void swf_referse_path(SWFPath *path)

```
....
536.                types[j] = path->types[path->nbType - i - 1];
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1330
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	3209	3209
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3209.                            odR->OD_ID[odR->NbODs] = id;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1331
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	3209	3209
Object	NbODs	NbODs

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3209.                            odR->OD_ID[odR->NbODs] = id;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1332
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	245	245
Object	j	j

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
245.                                  szLineConv[j] = 0xc0 | ( (szLine[i]
>> 6) & 0x3 );
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1333
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	251	251
Object	j	j

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
251.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1334
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	257	257
Object	j	j

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c

Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
257.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1335
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	260	260
Object	j	j

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c

Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
260.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1336
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	266	266
Object	j	j

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
266.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1337
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	269	269
Object	j	j

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
269.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17

	&pathid=1338
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	272	272
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
272.                                  szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1339
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Line	280	280
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
280.                        szLineConv[j] = szLine[i];
```

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=1000022&projectid=17&pathid=1220
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	558	567
Object	null	nalus

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
558.                pa = NULL;
....
567.          gf_list_add(pa->nalus, sl);
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1221
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	552	567
Object	null	nalus

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method	static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
567.        gf_list_add(pa->nalus, sl);
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1222
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c in line 49 is not initialized when it is used by Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c in line 49.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Line	211	211
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-37767-TP.c
Method static GF_Err BD_XReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
211.            * ((GF_ChildNodeItem **) targetField.far_ptr) = NULL;
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1223
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c in line 848 is not initialized when it is used by def_name at gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c in line 848.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c
Line	877	877
Object	null	def_name

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-41000-TP.c

Method GF_Err BM_SceneReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
877.                ri->def_name = r->name ? gf_strdup(r->name) : NULL;
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1224
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	270
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                      AVIAstream *st = NULL;
....
270.                      gf_filter_pid_set_property(st->opid,
GF_PROP_PID_STREAM_TYPE, &PROP_UINT(GF_STREAM_AUDIO) );
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1225
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	270
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                                st = NULL;
....
270.                        gf_filter_pid_set_property(st->opid,
GF_PROP_PID_STREAM_TYPE, &PROP_UINT(GF_STREAM_AUDIO) );
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1226
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	271
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                        AVIAstream *st = NULL;
....
271.                        gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CODECID, &PROP_UINT( codecid) );
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1227
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c

Line	258	271
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                          st = NULL;
....
271.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CODECID, &PROP_UINT( codecid) );
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1228
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	273
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                    AVIAstream *st = NULL;
....
273.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_SAMPLE_RATE, &PROP_UINT( st->freq ) );
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1229
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	273
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                              st = NULL;
....
273.                        gf_filter_pid_set_property(st->opid,
GF_PROP_PID_SAMPLE_RATE, &PROP_UINT( st->freq ) );
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1230
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	275
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                        AVIAstream *st = NULL;
....
275.                        gf_filter_pid_set_property(st->opid,
GF_PROP_PID_NUM_CHANNELS, &PROP_UINT( st->nb_channels ) );
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1231
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	275
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                          st = NULL;
....
275.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_NUM_CHANNELS, &PROP_UINT( st->nb_channels ) );
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1232
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	280
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                    AVIAstream *st = NULL;
....
280.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_ID, &PROP_UINT( 2 + st->stream_num) );
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1233
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	280
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                            st = NULL;
....
280.                      gf_filter_pid_set_property(st->opid,
GF_PROP_PID_ID, &PROP_UINT( 2 + st->stream_num) );
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1234
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	281
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                      AVIAstream *st = NULL;
....
281.                      gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CLOCK_ID, &PROP_UINT( sync_id ) );
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1235
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	281
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                                st = NULL;
....
281.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CLOCK_ID, &PROP_UINT( sync_id ) );
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1236
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	282
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                    AVIAstream *st = NULL;
....
282.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DURATION, &PROP_FRAC64( dur ) );
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1237
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	282
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                          st = NULL;
....
282.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DURATION, &PROP_FRAC64( dur ) );
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1238
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	284
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                          AVIAstream *st = NULL;
....
284.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_PLAYBACK_MODE, &PROP_UINT(GF_PLAYBACK_MODE_SEEK ) );
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1239
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	284
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                                 st = NULL;
....
284.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_PLAYBACK_MODE, &PROP_UINT(GF_PLAYBACK_MODE_SEEK ) );
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1240
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-	gpac@@gpac-v0.9.0-preview-CVE-2023-

	4678-TP.c	4678-TP.c
Line	258	287
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                          st = NULL;
....
287.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_UNFRAMED, &PROP_BOOL( GF_TRUE ) );
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1241
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	287
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                    AVIAstream *st = NULL;
....
287.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_UNFRAMED, &PROP_BOOL( GF_TRUE ) );
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1242
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	294
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                        AVIAstream *st = NULL;
....
294.                              gf_filter_pid_set_property(st->opid,
GF_PROP_PID_TIMESCALE, &PROP_UINT(st->freq) );
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1243
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	294
Object	null	opid

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                              st = NULL;
....
294.                              gf_filter_pid_set_property(st->opid,
GF_PROP_PID_TIMESCALE, &PROP_UINT(st->freq) );
```

NULL Pointer Dereference\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1244
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	308
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                             st = NULL;
....
308.                                   gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DECODER_CONFIG, &PROP_DATA_NO_COPY(dsi, dsi_len) );
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1245
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	308
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                       AVIAstream *st = NULL;
....
308.                                   gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DECODER_CONFIG, &PROP_DATA_NO_COPY(dsi, dsi_len) );
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1246
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	291
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                              st = NULL;
....
291.                                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_AUDIO_FORMAT, &PROP_UINT(afmt) );
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1247
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	291
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                    AVIAstream *st = NULL;
....
291.                                gf_filter_pid_set_property(st->opid,
GF_PROP_PID_AUDIO_FORMAT, &PROP_UINT(afmt) );
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1248
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	258	279
Object	null	opid

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c

Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                          st = NULL;
....
279.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_BITRATE, &PROP_UINT( brate ) );
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1249
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Line	253	279
Object	null	opid

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
253.                        AVIAstream *st = NULL;
....
279.                                gf_filter_pid_set_property(st->opid,
GF_PROP_PID_BITRATE, &PROP_UINT( brate ) );
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1250
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c in line 1243 is not initialized when it is used by have_dts at gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c
Line	1354	1119
Object	null	have_dts

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c
Method static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1354.                               add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c
Method static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                   (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1251
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c in line 1243 is not initialized when it is used by have_pts at gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c
Line	1354	1119
Object	null	have_pts

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c
Method static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1354.                         add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4681-TP.c

Method static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1252
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1271.        undef_node = NULL;
....
1327.        if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1253
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	1288	1327
Object	null	sgprivate

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1288.                              undef_node = NULL;
....
1327.        if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1254
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4683-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1512.                                   *(GF_ChildNodeItem **)info.far_ptr =
NULL;
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1255
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c in line 1243 is not initialized when it is used by have_dts at gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c
Line	1354	1119
Object	null	have_dts

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c
Method	static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1354.                             add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c
Method	static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1256
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c in line 1243 is not initialized when it is used by have_pts at gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c
Line	1354	1119
Object	null	have_pts

Code Snippet
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c
Method	static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1354.                              add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4721-TP.c
Method	static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                    (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1257
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1271.        undef_node = NULL;
....
1327.        if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1258
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	1288	1327
Object	null	sgprivate

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1288.                              undef_node = NULL;
....
1327.        if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1259
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4756-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1512.                                    *(GF_ChildNodeItem **)info.far_ptr =
NULL;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1260
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1271.        undef_node = NULL;
....
1327.        if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1261
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c

Line	1288	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1288.                               undef_node = NULL;
....
1327.        if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1262
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4778-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1512.                                    *(GF_ChildNodeItem **)info.far_ptr =
NULL;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1263
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	552	563
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.         GF_HEVCParamArray *pa = NULL;
....
563.               pa->type = nal_type;
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1264
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by array_completeness at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	552	562
Object	pa	array_completeness

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.         GF_HEVCParamArray *pa = NULL;
....
562.               pa->array_completeness = 1;
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1265
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	552	564
Object	pa	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
564.              pa->nalus = gf_list_new();
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1266
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	552	557
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
557.              if (pa->type == nal_type) break;
```

Potential Precision Problem

Query Path:
CPP\Cx\CPP Buffer Overflow\Potential Precision Problem Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Precision Problem\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1267
Status	New

The size of the buffer used by mp4_mux_format_report in "%s", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_format_report passes to "%s", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4288	4288
Object	"%s"	"%s"

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c

Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4288.                     sprintf(szStatus, "%s", ((ctx-
>store==MP4MX_MODE_FLAT) || (ctx->store==MP4MX_MODE_FASTSTART)) ? "mux"
: "import");
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1268
Status	New

The size of the buffer used by mp4_mux_format_report in " %s%d(%c): %d %%", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_format_report passes to " %s%d(%c): %d %%", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Line	4333	4333

Object	" %s%d(%c): %d %%"	" %s%d(%c): %d %%"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47654-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4333.                           sprintf(szTK, " %s%d(%c): %d %%", tkw-
>is_item ? "IT" : "TK", tkw->track_id, tkw->status_type, pc/100);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1269
Status	New

The size of the buffer used by naludmx_process in "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_process passes to "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Line	2890	2890
Object	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P %
8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx-
>height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1270
Status	New

The size of the buffer used by mp3_dmx_flush_id3 in "tag:%s", at line 207 of gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp3_dmx_flush_id3 passes to "tag:%s", at line 207 of gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Line	315	315
Object	"tag:%s"	"tag:%s"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-3291-TP.c
Method static void mp3_dmx_flush_id3(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
315.                        sprintf(szTag, "tag:%s", gf_4cc_to_str(ftag));
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1271
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s%c%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_sm_load_init_swf passes to "%s%c%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2660	2660
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2660.                        sprintf(svgFileName, "%s%c%s.svg", load-
>localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1272
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_sm_load_init_swf passes to "%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2662	2662
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2662.                          sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1273
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_soundstream_hdr passes to "%s/swf_soundstream_%d.mp3", at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	1960	1960
Object	"%s/swf_soundstream_%d.mp3"	"%s/swf_soundstream_%d.mp3"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.                    sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Potential Precision Problem\Path 8:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1274
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_jpeg_%d.jpg", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_def_bits_jpeg passes to "%s/swf_jpeg_%d.jpg", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2073	2073
Object	"%s/swf_jpeg_%d.jpg"	"%s/swf_jpeg_%d.jpg"

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2073.            sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1275
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_png_%d.png", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_def_bits_jpeg passes to "%s/swf_png_%d.png", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c
Line	2149	2149
Object	"%s/swf_png_%d.png"	"%s/swf_png_%d.png"

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2023-46426-TP.c

Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2149.                sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1276
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s%c%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_sm_load_init_swf passes to "%s%c%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2660	2660
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2660.                         sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1277
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_sm_load_init_swf passes to "%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2662	2662
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2662.                    sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1278
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_soundstream_hdr passes to "%s/swf_soundstream_%d.mp3", at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	1960	1960
Object	"%s/swf_soundstream_%d.mp3"	"%s/swf_soundstream_%d.mp3"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.                    sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1279
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_jpeg_%d.jpg", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_def_bits_jpeg passes to "%s/swf_jpeg_%d.jpg", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2073	2073

Object	"%s/swf_jpeg_%d.jpg"	"%s/swf_jpeg_%d.jpg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2073.           sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath, ID);
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1280
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_png_%d.png", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_def_bits_jpeg passes to "%s/swf_png_%d.png", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Line	2149	2149
Object	"%s/swf_png_%d.png"	"%s/swf_png_%d.png"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2149.                   sprintf(szName, "%s/swf_png_%d.png", read->localPath, ID);
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1281
Status	New

The size of the buffer used by mp4_mux_format_report in "%s", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_format_report passes to "%s", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4288	4288
Object	"%s"	"%s"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4288.                         sprintf(szStatus, "%s", ((ctx-
>store==MP4MX_MODE_FLAT) || (ctx->store==MP4MX_MODE_FASTSTART)) ? "mux"
: "import");
```

Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1282
Status	New

The size of the buffer used by mp4_mux_format_report in " %s%d(%c): %d %%", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_format_report passes to " %s%d(%c): %d %%", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Line	4333	4333
Object	" %s%d(%c): %d %%"	" %s%d(%c): %d %%"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4722-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4333.                               sprintf(szTK, " %s%d(%c): %d %%", tkw-
>is_item ? "IT" : "TK", tkw->track_id, tkw->status_type, pc/100);
```

Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1283
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s%c%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_sm_load_init_swf passes to "%s%c%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2660	2660
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2660.                          sprintf(svgFileName, "%s%c%s.svg", load-
>localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1284
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_sm_load_init_swf passes to "%s.svg", at line 2616 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2662	2662
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2662.                          sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Potential Precision Problem\Path 19:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1285
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_soundstream_hdr passes to "%s/swf_soundstream_%d.mp3", at line 1920 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	1960	1960
Object	"%s/swf_soundstream_%d.mp3"	"%s/swf_soundstream_%d.mp3"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.                    sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1286
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_jpeg_%d.jpg", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_def_bits_jpeg passes to "%s/swf_jpeg_%d.jpg", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2073	2073
Object	"%s/swf_jpeg_%d.jpg"	"%s/swf_jpeg_%d.jpg"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2073.              sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1287
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_png_%d.png", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that swf_def_bits_jpeg passes to "%s/swf_png_%d.png", at line 2052 of gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Line	2149	2149
Object	"%s/swf_png_%d.png"	"%s/swf_png_%d.png"

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4754-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2149.                 sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Potential Precision Problem\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1288
Status	New

The size of the buffer used by mp4_mux_format_report in "%s", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_format_report passes to "%s", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	4288	4288
Object	"%s"	"%s"

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method	void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4288.                    sprintf(szStatus, "%s", ((ctx-
>store==MP4MX_MODE_FLAT) || (ctx->store==MP4MX_MODE_FASTSTART)) ? "mux"
: "import");
```

Potential Precision Problem\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1289
Status	New

The size of the buffer used by mp4_mux_format_report in " %s%d(%c): %d %%", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mp4_mux_format_report passes to " %s%d(%c): %d %%", at line 4245 of gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Line	4333	4333
Object	" %s%d(%c): %d %%"	" %s%d(%c): %d %%"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2023-4755-TP.c
Method void mp4_mux_format_report(GF_Filter *filter, GF_MP4MuxCtx *ctx, u64 done, u64 total)

```
....
4333.                    sprintf(szTK, " %s%d(%c): %d %%", tkw-
>is_item ? "IT" : "TK", tkw->track_id, tkw->status_type, pc/100);
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1218
Status	New

The buffer allocated by <= in gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c at line 76 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Line	116	116
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Method static Bool latm_dmx_sync_frame_bs(GF_BitStream *bs, GF_M4ADecSpecInfo *acfg, u32 *nb_bytes, u8 *buffer, u32 *nb_skipped)

```
....
116.                             for (i=0; i<=numProgram; i++) {
```

Potential Off by One Error in Loops\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000022&projectid=17&pathid=1219
Status New

The buffer allocated by <= in gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c at line 76 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Line	119	119
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47659-TP.c
Method static Bool latm_dmx_sync_frame_bs(GF_BitStream *bs, GF_M4ADecSpecInfo *acfg, u32 *nb_bytes, u8 *buffer, u32 *nb_skipped)

```
....
119.                                   for (j=0; j<=num_lay; j++) {
```

Buffer Overflow cpycat

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 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

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```java
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
      if (count > 0)
            return total / count;
      else
            return 0;
}
```

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

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 Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

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	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

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, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

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';
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699** **Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-10-29	Unchecked Array Indexing

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025