vul_files_17 Scan Report

Project Name	vul_files_17
Scan Start	Monday, January 6, 2025 11:05:46 PM
Preset	Checkmarx Default
Scan Time	02h:45m:28s
Lines Of Code Scanned	299410
Files Scanned	76
Report Creation Time	Tuesday, January 7, 2025 10:15:26 AM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19
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

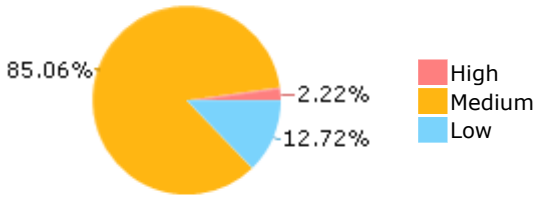
Results Limit

Results limit per query was set to 50

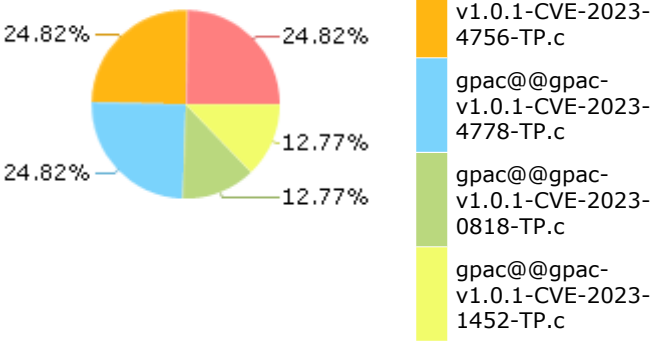
Selected Queries

Selected queries are listed in Result Summary

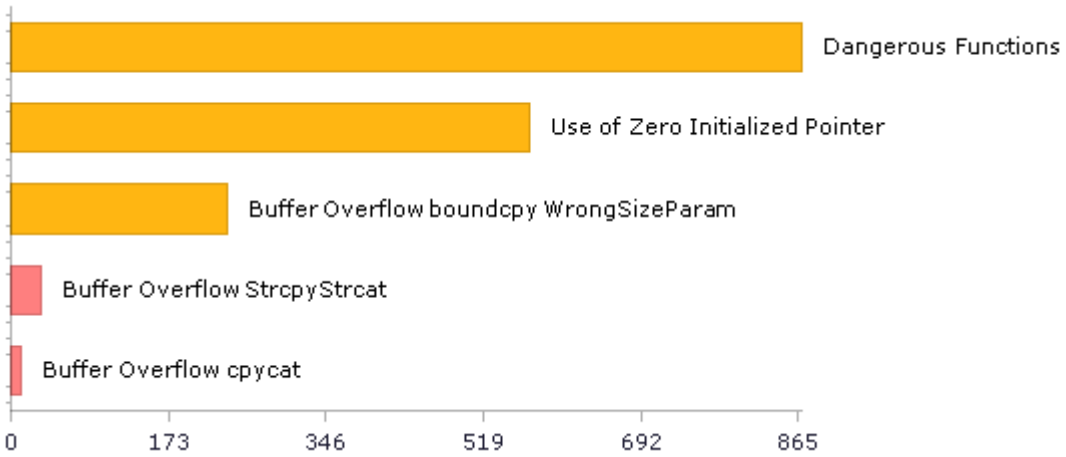
Result Summary



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	403	288
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	26	26
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	869	869
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	869	869
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	284	252
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.	26	26
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)	26	26
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)*	669	72
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	130	100
SI-11 Error Handling (P2)*	40	40
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

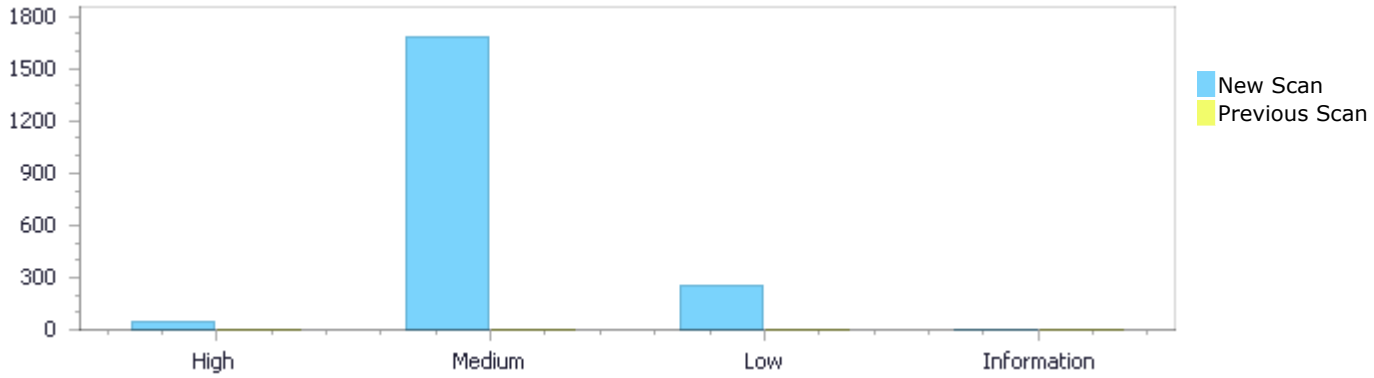
Scan Summary - Custom

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	44	1,685	252	0	1,981
Recurrent Issues	0	0	0	0	0
Total	44	1,685	252	0	1,981
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	44	1,685	252	0	1,981
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	44	1,685	252	0	1,981

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	32	High
Buffer Overflow cpycat	12	High
Dangerous Functions	869	Medium
Use of Zero Initialized Pointer	570	Medium
Buffer Overflow boundcpy WrongSizeParam	237	Medium

Divide By Zero	5	Medium
Buffer Overflow Loops	3	Medium
Use of Uninitialized Variable	1	Medium
NULL Pointer Dereference	98	Low
Unchecked Array Index	67	Low
Unchecked Return Value	40	Low
Improper Resource Access Authorization	26	Low
Potential Precision Problem	19	Low
Potential Off by One Error in Loops	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	235
gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	235
gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	235
gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	114
gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	114
gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	114
gpac@@gpac-v1.0.1-CVE-2024-6062-TP.c	114
gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c	76
gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	63
gpac@@gpac-v1.0.1-CVE-2023-4720-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=1000025&projectid=19&pathid=13
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=14
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=15
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=16
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=17
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=18
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c

Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=19
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=20
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=21
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=22
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=23
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=24
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=25

Status New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 232 of gpac@@gpac-v1.0.1-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 232 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	232	310
Object	szLine	szLine

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c

Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

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

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=26
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 232 of gpac@@gpac-v1.0.1-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 232 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	232	310
Object	szLine	szLine

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c

Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

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

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=27
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c

Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=28
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=29
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=30
Status New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=31
Status New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=32
Status New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=33
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 232 of gpac@@gpac-v1.0.1-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 232 of gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Line	232	310
Object	szLine	szLine

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

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

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=34
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 232 of gpac@@gpac-v1.0.1-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 232 of gpac@@gpac-v1.0.1-CVE-2024-6062-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-6062-TP.c	gpac@@gpac-v1.0.1-CVE-2024-6062-TP.c
Line	232	310
Object	szLine	szLine

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-6062-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

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

Buffer Overflow StrcpyStrcat\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=35
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4269
Object	mpd_src	item_path

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void revert_cache_file(char *item_path)

```
....
4269.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=36
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack,

using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4269
Object	output_dir	item_path

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void revert_cache_file(char *item_path)

```
....
4269.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 25:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=37
Status New

The size of the buffer used by revert_cache_file in item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that revert_cache_file passes to item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4256	4269
Object	item_path	item_path

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void revert_cache_file(char *item_path)

```
....
4256.  static void revert_cache_file(char *item_path)
....
4269.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=38
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4270
Object	mpd_src	szPATH

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Method static void revert_cache_file(char *item_path)

```
....
4270.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=39
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4270

Object	output_dir	szPATH

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Method static void revert_cache_file(char *item_path)

```
....
4270.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=40
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that revert_cache_file passes to item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4256	4270
Object	item_path	szPATH

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void revert_cache_file(char *item_path)

```
....
4256.  static void revert_cache_file(char *item_path)
....
4270.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=41

Status	New

The size of the buffer used by rip_mpd in sess, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4353
Object	mpd_src	sess

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
4353.       strcpy(szName, gf_dm_sess_get_cache_name(sess) );
```

Buffer Overflow StrcpyStrcat\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=42
Status	New

The size of the buffer used by rip_mpd in gf_dm_sess_get_cache_name, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4353
Object	mpd_src	gf_dm_sess_get_cache_name

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
4353.       strcpy(szName, gf_dm_sess_get_cache_name(sess) );
```

Buffer Overflow StrcpyStrcat\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=43
Status	New

The size of the buffer used by rip_mpd in output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4328
Object	output_dir	output_dir

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
4328.              strcpy(szName, output_dir);
```

Buffer Overflow StrcpyStrcat\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=44
Status	New

The size of the buffer used by rip_mpd in szName, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4313	4353
Object	output_dir	szName

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4313.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
4353.       strcpy(szName, gf_dm_sess_get_cache_name(sess) );
```

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=1000025&projectid=19&pathid=1
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=2
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=3
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c

Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=4
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=5
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=6
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=7
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=8
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=9
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=10
Status New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=11
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=12
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v1.0.1-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-v1.0.1-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=1000025&projectid=19&pathid=290
Status	New

The dangerous function, memcpy, was found in use at line 422 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47659-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Line	467	467
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=291
Status	New

The dangerous function, memcpy, was found in use at line 422 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47659-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Line	510	510
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=292
Status	New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	435	435
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=293
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	445	445
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=294
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	453	453
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=295
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	501	501
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=296
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	506	506
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=297
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	562	562
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=298
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	573	573
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=299
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	579	579
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=300
Status New

The dangerous function, memcpy, was found in use at line 357 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47663-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Line	581	581
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=301
Status New

The dangerous function, memcpy, was found in use at line 933 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	955	955
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static void gf_webvtt_flush_sample(void *user, GF_WebVTTSample *samp)

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

Dangerous Functions\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=302
Status New

The dangerous function, memcpy, was found in use at line 1431 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	1587	1587
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err gf_text_process_ttml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1587.                    memcpy(pck_data, txt_str, txt_len);
```

Dangerous Functions\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=303
Status New

The dangerous function, memcpy, was found in use at line 1612 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	1626	1626
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1626.        memcpy(pck_data, data, length);
```

Dangerous Functions\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=304
Status New

The dangerous function, memcpy, was found in use at line 1638 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	1651	1651
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err swf_svg_add_iso_header(void *user, const u8 *data, u32 length, Bool isHeader)

```
....
1651.             memcpy(pck_data, data, length);
```

Dangerous Functions\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=305
Status New

The dangerous function, memcpy, was found in use at line 496 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0866-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Line	551	551
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=306
Status New

The dangerous function, memcpy, was found in use at line 496 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0866-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Line	592	592
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

```
....
592.                        memcpy(ctx->id3_buffer, start, 10);
```

Dangerous Functions\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=307
Status New

The dangerous function, memcpy, was found in use at line 496 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0866-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Line	605	605
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

```
....
605.                    memcpy(ctx->id3_buffer + ctx->id3_buffer_size,
start, bytes_to_drop);
```

Dangerous Functions\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=308
Status New

The dangerous function, memcpy, was found in use at line 496 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-0866-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Line	715	715
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=309
Status	New

The dangerous function, memcpy, was found in use at line 715 in gpac@@gpac-v1.0.1-CVE-2023-1449-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-v1.0.1-CVE-2023-1449-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Line	734	734
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Method static GF_Err av1dmx_parse_flush_sample(GF_Filter *filter, GF_AV1DmxCtx *ctx)

```
....
734.        memcpy(output, ctx->state.frame_obus, pck_size);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=310
Status	New

The dangerous function, memcpy, was found in use at line 867 in gpac@@gpac-v1.0.1-CVE-2023-1449-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-v1.0.1-CVE-2023-1449-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Line	930	930
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

```
....
930.                    memcpy(ctx->buffer+ctx->buf_size, data,
pck_size);
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=311
Status New

The dangerous function, memcpy, was found in use at line 867 in gpac@@gpac-v1.0.1-CVE-2023-1449-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-v1.0.1-CVE-2023-1449-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Line	962	962
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

```
....
962.                    memcpy(ctx->buffer+ctx->buf_size, data,
pck_size);
```

Dangerous Functions\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=312
Status New

The dangerous function, memcpy, was found in use at line 867 in gpac@@gpac-v1.0.1-CVE-2023-1449-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-v1.0.1-CVE-2023-1449-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Line	980	980
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1449-TP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

```
....
980.        memcpy(ctx->buffer+ctx->buf_size, data, pck_size);
```

Dangerous Functions\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=313
Status New

The dangerous function, memcpy, was found in use at line 933 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	955	955
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static void gf_webvtt_flush_sample(void *user, GF_WebVTTSample *samp)

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

Dangerous Functions\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=314
Status New

The dangerous function, memcpy, was found in use at line 1431 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	1587	1587
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err gf_text_process_ttml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1587.                    memcpy(pck_data, txt_str, txt_len);
```

Dangerous Functions\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=315
Status New

The dangerous function, memcpy, was found in use at line 1612 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	1626	1626
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1626.        memcpy(pck_data, data, length);
```

Dangerous Functions\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=316
Status New

The dangerous function, memcpy, was found in use at line 1638 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	1651	1651
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err swf_svg_add_iso_header(void *user, const u8 *data, u32 length, Bool isHeader)

```
....
1651.             memcpy(pck_data, data, length);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=317
Status	New

The dangerous function, memcpy, was found in use at line 1413 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1485	1485
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1485.             memcpy(sl->data, data, size);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=318
Status	New

The dangerous function, memcpy, was found in use at line 1413 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1500	1500
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1500.       memcpy(sl->data, data, size);
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=319
Status	New

The dangerous function, memcpy, was found in use at line 1867 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1931	1931
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1931.                   memcpy(ctx->sei_buffer + ctx->sei_buffer_size +
ctx->nal_length, data, sei_size);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=320
Status	New

The dangerous function, memcpy, was found in use at line 1867 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1955	1955
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1955.                    memcpy(ctx->init_aud, data, 2);
```

Dangerous Functions\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=321
Status New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2154	2154
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2154.              memcpy(ctx->hdr_store + ctx->hdr_store_size, data,
sizeof(char)*pck_size);
```

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=322
Status New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2234	2234
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2234.                    memcpy(ctx->hdr_store, start, remain);
```

Dangerous Functions\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=323
Status New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2245	2245
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2245.                    memcpy(ctx->hdr_store + ctx->bytes_in_header,
start, SAFETY_NAL_STORE - ctx->bytes_in_header);
```

Dangerous Functions\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=324
Status New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2255	2255
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2255.                                          memcpy(pck_data, ctx-
>hdr_store, ctx->bytes_in_header);
```

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=325
Status New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2353	2353
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2353.                                          memcpy(pck_data, start,
(size_t) size);
```

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=326

Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2357	2357
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2357.                                   memcpy(ctx->hdr_store, start+remain-
3, 3);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=327
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2400	2400
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2400.                                   memcpy(pck_data, ctx->hdr_store,
current);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19

	&pathid=328
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2404	2404
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2404.                                   memcpy(pck_data, start, current);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=329
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2503	2503
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2503.                                   memcpy(ctx->hdr_store + ctx-
>hdr_store_size, start, sizeof(char)*pck_avail);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19

	&pathid=330
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2542	2542
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2542.                                                memcpy(ctx->hdr_store +
hdr_offset + nal_bytes_from_store, start, copy_size);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=331
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2555	2555
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2555.                                    memcpy(ctx->hdr_store, start,
remain);
```

Dangerous Functions\Path 43:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=332
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2602	2602
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2602.                                   memcpy(ctx->hdr_store, start+remain-
3, 3);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=333
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2742	2742
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2742.                                   memcpy(ctx->svc_prefix_buffer,
start+sc_size, ctx->svc_prefix_buffer_size);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=334
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2940	2940
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2940.                    memcpy(pck_data + ctx->nal_length , ctx-
>init_aud, audelim_size);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=335
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2949	2949
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2949.                    memcpy(pck_data, ctx->sei_buffer, ctx-
>sei_buffer_size);
```

Dangerous Functions\Path 47:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=336
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2958	2958
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2958.                    memcpy(pck_data + ctx->nal_length, ctx->svc_prefix_buffer, ctx->svc_prefix_buffer_size);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=337
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2976	2976
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2976.                    memcpy(pck_data, hdr_start, nal_bytes_from_store);
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=338
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2980	2980
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2980.                           memcpy(pck_data + nal_bytes_from_store,
pck_start, (size_t) size);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=339
Status	New

The dangerous function, memcpy, was found in use at line 2087 in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	2992	2992
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2992.                   memcpy(pck_data, pck_start, (size_t) 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=1000025&projectid=19&pathid=1386
Status	New

The variable declared in avc_state at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 322 is not initialized when it is used by avc_state at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 322.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	327	435
Object	avc_state	avc_state

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

```
....
327.        AVCState *avc_state = NULL;
....
435.                    nal_type = avc_state->last_nal_type_parsed;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1387
Status	New

The variable declared in pa at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 628 is not initialized when it is used by pa at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 628.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	636	647
Object	pa	pa

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method	static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
636.                pa = NULL;
....
647.        gf_list_add(pa->nalus, sl);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1388
Status	New

The variable declared in pa at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 628 is not initialized when it is used by pa at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 628.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	630	647
Object	pa	pa

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method	static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1389
Status	New

The variable declared in buf at gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c in line 215 is not initialized when it is used by buf at gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c in line 215.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c

Line	219	254
Object	buf	buf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Method void id3dmx_flush(GF_Filter *filter, u8 *id3_buf, u32 id3_buf_size, GF_FilterPid *audio_pid, GF_FilterPid **video_pid_p)

```
....
219.        char *buf=NULL;
....
254.                    buf = gf_realloc(buf, fsize+2);
```

Use of Zero Initialized Pointer\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1390
Status New

The variable declared in offset_table at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 1418 is not initialized when it is used by offset_table at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 1418.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1423	1489
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1423.       u32 *offset_table = NULL;
....
1489.                           e = swf_seek_file_to(read, start +
offset_table[i]);
```

Use of Zero Initialized Pointer\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1391
Status New

The variable declared in st at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by st at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	270
Object	st	st

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            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 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1392
Status New

The variable declared in st at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by st at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	270
Object	st	st

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    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 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1393
Status New

The variable declared in offset_table at gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c in line 1418 is not initialized when it is used by offset_table at gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c in line 1418.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1423	1489
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1423.       u32 *offset_table = NULL;
....
1489.                           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=1000025&projectid=19&pathid=1394
Status New

The variable declared in offset_table at gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c in line 1418 is not initialized when it is used by offset_table at gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c in line 1418.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1423	1489
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1423.       u32 *offset_table = NULL;
....
1489.                           e = swf_seek_file_to(read, start +
offset_table[i]);
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1395
Status	New

The variable declared in a at gpac@@gpac-v2.0.0-CVE-2020-19488-FP.c in line 104 is not initialized when it is used by a at gpac@@gpac-v2.0.0-CVE-2020-19488-FP.c in line 104.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-19488-FP.c	gpac@@gpac-v2.0.0-CVE-2020-19488-FP.c
Line	108	128
Object	a	a

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-19488-FP.c
Method GF_Err ilst_item_box_read(GF_Box *s,GF_BitStream *bs)

```
....
108.        GF_Box *a = NULL;
....
128.              ISOM_DECREASE_SIZE(ptr, a->size);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1396
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 857 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	990	1427
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

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

File Name	gpac@@gpac-v1.0.1-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)

```
....
1427.                   list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1397
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1025 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1158	1427
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v1.0.1-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)

```
....
1158.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v1.0.1-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)

```
....
1427.                   list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1398
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1025 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1158	1440
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v1.0.1-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)

```
....
1158.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1440.                   list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1399
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 857 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	990	1440
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v1.0.1-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)

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

File Name	gpac@@gpac-v1.0.1-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)

```
....
1440.                   list = ctx->sps;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1400
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1604 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1636.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1610	1647
Object	Pointer	first_pck_in_au

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method	GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1610.        *data_ptr = NULL;
```

File Name	gpac@@gpac-v1.0.1-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)

```
....
1647.              ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1401
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 857 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1636.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	990	1647
Object	Pointer	first_pck_in_au

Code Snippet

File Name gpac@@gpac-v1.0.1-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)

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

File Name gpac@@gpac-v1.0.1-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)

```
....
1647.            ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1402
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1025 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1636.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1158	1647

Object	Pointer	first_pck_in_au

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1158.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1647.             ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1403
Status	New

The variable declared in first_pck_in_au at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1509 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1636.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1590	1647
Object	first_pck_in_au	first_pck_in_au

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method void naludmx_finalize_au_flags(GF_NALUDmxCtx *ctx)

```
....
1590.       ctx->first_pck_in_au = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1647.             ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1404
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1604 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1610	1430
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c

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

```
....
1610.       *data_ptr = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1430.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1405
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1025 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination

File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1158	1430
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1158.        *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1430.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1406
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 857 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	990	1430
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

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

File Name	gpac@@gpac-v1.0.1-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)

```
....
1430.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1407
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1604 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1610	1443
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method	GF_Err naludmx_realloc_last_pck(GF_NALUDmxCtx *ctx, u32 nb_bytes_to_add, u8 **data_ptr)

```
....
1610.       *data_ptr = NULL;
```

File Name	gpac@@gpac-v1.0.1-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)

```
....
1443.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1408
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1025 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1158	1443
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

```
....
1158.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1443.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1409
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 857 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	990	1443
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v1.0.1-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)

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

File Name gpac@@gpac-v1.0.1-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)

```
....
1443.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1410
Status	New

The variable declared in Pointer at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1604 is not initialized when it is used by list at gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c in line 1413.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	1610	1448
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c

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

```
....
1610.        *data_ptr = NULL;
```

File Name gpac@@gpac-v1.0.1-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)

```
....
1448.                   list = ctx->sps_ext;
```

Use of Zero Initialized Pointer\Path 26:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1411
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365 is not initialized when it is used by ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	375	385
Object	ActiveQP	ActiveQP

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
375.        codec->ActiveQP = NULL;
....
385.        codec->ActiveQP = (M_QuantizationParameter *) node;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1412
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365 is not initialized when it is used by ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	373	385
Object	global_qp	ActiveQP

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
373.              codec->scenegraph->global_qp = NULL;
....
385.        codec->ActiveQP = (M_QuantizationParameter *) node;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1413
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365 is not initialized when it is used by global_qp at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	375	383
Object	ActiveQP	global_qp

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
375.        codec->ActiveQP = NULL;
....
383.        codec->scenegraph->global_qp = node;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1414
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365 is not initialized when it is used by global_qp at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 365.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	373	383
Object	global_qp	global_qp

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
373.              codec->scenegraph->global_qp = NULL;
....
383.        codec->scenegraph->global_qp = node;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1415
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 399.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	433
Object	ActiveQP	new_node

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method GF_Err BM_ParseNodeInsert(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
433.              inf->new_node = node;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1416
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 399.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	433
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method GF_Err BM_ParseNodeInsert(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
433.              inf->new_node = node;
```

Use of Zero Initialized Pointer\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1417
Status New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 43.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	77
Object	ActiveQP	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
```

File Name	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method	static GF_Err BM_ParseMultipleIndexedReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
77.                inf->new_node = gf_bifs_dec_node(codec, bs,
field.NDTtype);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1418
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 43.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	77
Object	global_qp	new_node

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method	static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
```

File Name	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method	static GF_Err BM_ParseMultipleIndexedReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
77.                inf->new_node = gf_bifs_dec_node(codec, bs,
field.NDTtype);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1419
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 444.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	498
Object	ActiveQP	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method GF_Err BM_ParseIndexInsert(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
498.                    inf->new_node = node;
```

Use of Zero Initialized Pointer\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1420
Status New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 444.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	498
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method GF_Err BM_ParseIndexInsert(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
498.                    inf->new_node = node;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1421
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 670.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	685
Object	ActiveQP	new_node

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method GF_Err BM_ParseNodeReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
685.        inf->new_node = gf_bifs_dec_node(codec, bs,
NDT_SFWorldNode);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1422
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 670.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	685
Object	global_qp	new_node

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method GF_Err BM_ParseNodeReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
685.        inf->new_node = gf_bifs_dec_node(codec, bs,
NDT_SFWorldNode);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1423
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 732.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	779
Object	ActiveQP	new_node

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method GF_Err BM_ParseIndexValueReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
779.              inf->new_node = gf_bifs_dec_node(codec, bs,
field.NDTtype);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1424
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 732.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	779
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Method GF_Err BM_ParseIndexValueReplace(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
779.              inf->new_node = gf_bifs_dec_node(codec, bs,
field.NDTtype);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1425
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	195
Object	ActiveQP	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
....
195.        inf->new_node = node;
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1426
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	195
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
....
195.        inf->new_node = node;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1427
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	188
Object	ActiveQP	global_qp

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
....
188.        codec->scenegraph->global_qp = node;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1428
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	178	188
Object	global_qp	global_qp

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
....
188.        codec->scenegraph->global_qp = node;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1429
Status	New

The variable declared in ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	177	186
Object	ActiveQP	ActiveQP

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
177.        codec->ActiveQP = NULL;
....
186.        codec->ActiveQP = (M_QuantizationParameter *) node;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1430
Status	New

The variable declared in global_qp at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by ActiveQP at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Line	178	186
Object	global_qp	ActiveQP

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

```
....
178.        codec->scenegraph->global_qp = NULL;
....
186.        codec->ActiveQP = (M_QuantizationParameter *) node;
```

Use of Zero Initialized Pointer\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1431
Status New

The variable declared in localPath at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 2538 is not initialized when it is used by sound_stream at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 1922.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2565	1960
Object	localPath	sound_stream

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method SWFReader *gf_swf_reader_new(const char *localPath, const char *inputName)

```
....
2565.                    read->localPath = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.             read->sound_stream = snd;
```

Use of Zero Initialized Pointer\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19

	&pathid=1432
Status	New

The variable declared in sound_stream at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 1731 is not initialized when it is used by sound_stream at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 1922.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1737	1960
Object	sound_stream	sound_stream

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static void swf_delete_sound_stream(SWFReader *read)

```
....
1737.       read->sound_stream = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1960.             read->sound_stream = snd;
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1433
Status	New

The variable declared in loader_priv at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 2526 is not initialized when it is used by loader_priv at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 2526.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2535	2528
Object	loader_priv	loader_priv

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method void gf_sm_load_done_swf(GF_SceneLoader *load)

```
....
2535.       load->loader_priv = NULL;
....
2528.       SWFReader *read = (SWFReader *) load->loader_priv;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1434
Status	New

The variable declared in localPath at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 2538 is not initialized when it is used by loader_priv at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 2526.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2565	2528
Object	localPath	loader_priv

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c

Method SWFReader *gf_swf_reader_new(const char *localPath, const char *inputName)

```
....
2565.                   read->localPath = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c

Method void gf_sm_load_done_swf(GF_SceneLoader *load)

```
....
2528.       SWFReader *read = (SWFReader *) load->loader_priv;
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1435
Status	New

The variable declared in localPath at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 2538 is not initialized when it is used by offset_table at gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c in line 1418.

	Source	Destination

File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2565	1445
Object	localPath	offset_table

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method SWFReader *gf_swf_reader_new(const char *localPath, const char *inputName)

```
....
2565.                    read->localPath = NULL;
```

File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_font(SWFReader *read, u32 revision)

```
....
1445.                    e = swf_seek_file_to(read, start +
offset_table[i]);
```

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=1000025&projectid=19&pathid=50
Status	New

The size of the buffer used by BD_XReplace in GF_FieldInfo, at line 49 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	180	180
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v1.0.1-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 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=51
Status	New

The size of the buffer used by BD_DecMultipleIndexReplace in GF_FieldInfo, at line 285 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	325	325
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=52
Status	New

The size of the buffer used by BD_DecIndexInsert in GF_FieldInfo, at line 581 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	620	620
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=53
Status	New

The size of the buffer used by BD_DecIndexValueReplace in GF_FieldInfo, at line 827 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	883	883
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=54
Status	New

The size of the buffer used by BM_ParseIndexInsert in GF_FieldInfo, at line 444 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-41000-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c

Line	485	485
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v1.0.1-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 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=55
Status New

The size of the buffer used by BM_ParseIndexValueReplace in GF_FieldInfo, at line 732 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-41000-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	783	783
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v1.0.1-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 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=56
Status New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v1.0.1-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 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=57
Status New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1364	1364
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1364.                           memcpy(&mat, &ds->mat,
sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=58
Status New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1368	1368
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1368.                           memcpy(&cmat, &ds->cmat,
sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=59
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1387	1387
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1387.       memcpy(&ds->mat, &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=1000025&projectid=19&pathid=60
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1388	1388
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1388.       memcpy(&ds->cmat, &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=1000025&projectid=19&pathid=61
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v1.0.1-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 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=62
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1364	1364
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1364.                           memcpy(&mat, &ds->mat,
sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=63
Status New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1368	1368
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1368.                           memcpy(&cmat, &ds->cmat,
sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=64
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1387	1387
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1387.       memcpy(&ds->mat, &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=1000025&projectid=19&pathid=65
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1388	1388
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1388.       memcpy(&ds->cmat, &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=1000025&projectid=19&pathid=66
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v1.0.1-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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=67
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1364	1364
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1364.                           memcpy(&mat, &ds->mat,
sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=68
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1368	1368
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1368.                           memcpy(&cmat, &ds->cmat,
sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=69
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1387	1387
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1387.       memcpy(&ds->mat, &mat, sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=70
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v1.0.1-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 1247 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1388	1388
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

```
....
1388.       memcpy(&ds->cmat, &cmat, sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=71
Status	New

The size of the buffer used by isor_reader_get_sample in bin128, at line 201 of gpac@@gpac-v1.0.1-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 201 of gpac@@gpac-v1.0.1-CVE-2023-48013-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-48013-TP.c	gpac@@gpac-v1.0.1-CVE-2023-48013-TP.c
Line	493	493
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-48013-TP.c
Method void isor_reader_get_sample(ISOMChannel *ch)

```
....
493.                                    memcpy(ch->KID, KID,
sizeof(bin128));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=72
Status	New

The size of the buffer used by latm_dmx_check_dur in GF_M4ADecSpecInfo, at line 215 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47659-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Line	243	243
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v1.0.1-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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=73
Status	New

The size of the buffer used by ttxt_parse_text_box in GF_BoxRecord, at line 1895 of gpac@@gpac-v1.0.1-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 1895 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	1899	1899
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	static void ttxt_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
1899.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=74
Status	New

The size of the buffer used by ttxt_parse_text_style in GF_StyleRecord, at line 1908 of gpac@@gpac-v1.0.1-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 1908 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	1912	1912
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	static void ttxt_parse_text_style(GF_TXTIn *ctx, GF_XMLNode *n, GF_StyleRecord *style)

```
....
1912.       memset(style, 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=75
Status	New

The size of the buffer used by txtin_setup_ttxt in GF_TextSampleDescriptor, at line 1931 of gpac@@gpac-v1.0.1-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 1931 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	2017	2017
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	static GF_Err txtin_setup_ttxt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2017.                                   memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=76
Status	New

The size of the buffer used by tx3g_parse_text_box in GF_BoxRecord, at line 2341 of gpac@@gpac-v1.0.1-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 2341 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	2345	2345
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	static void tx3g_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
2345.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=77
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c

Line	2475	2475
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2475.             memset(&td, 0, sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=78
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	2498	2498
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2498.                         memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=79
Status	New

The size of the buffer used by txtin_process_texml in GF_StyleRecord, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	2565	2565
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2565.
      memset(&styles[nb_styles], 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=80
Status	New

The size of the buffer used by txtin_process_texml in Marker, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	2683	2683
Object	Marker	Marker

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2683.
      memset(&marks[nb_marks], 0, sizeof(Marker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=81
Status	New

The size of the buffer used by adts_dmx_check_pid in GF_M4ADecSpecInfo, at line 265 of gpac@@gpac-v1.0.1-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 265 of gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Line	337	337
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Method static void adts_dmx_check_pid(GF_Filter *filter, GF_ADTSDmxCtx *ctx)

```
....
337.        memset(&acfg, 0, sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=82
Status New

The size of the buffer used by *adts_dmx_probe_data in ADTSHeader, at line 780 of gpac@@gpac-v1.0.1-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 780 of gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Line	805	805
Object	ADTSHeader	ADTSHeader

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0866-TP.c
Method static const char *adts_dmx_probe_data(const u8 *data, u32 size, GF_FilterProbeScore *score)

```
....
805.        memset(&prev_hdr, 0, sizeof(ADTSHeader));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=83

Status	New

The size of the buffer used by ttxt_parse_text_box in GF_BoxRecord, at line 1895 of gpac@@gpac-v1.0.1-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 1895 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	1899	1899
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static void ttxt_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
1899.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=84
Status	New

The size of the buffer used by ttxt_parse_text_style in GF_StyleRecord, at line 1908 of gpac@@gpac-v1.0.1-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 1908 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	1912	1912
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static void ttxt_parse_text_style(GF_TXTIn *ctx, GF_XMLNode *n, GF_StyleRecord *style)

```
....
1912.       memset(style, 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=85
Status	New

The size of the buffer used by txtin_setup_ttxt in GF_TextSampleDescriptor, at line 1931 of gpac@@gpac-v1.0.1-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 1931 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	2017	2017
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err txtin_setup_ttxt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2017.                                   memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=86
Status	New

The size of the buffer used by tx3g_parse_text_box in GF_BoxRecord, at line 2341 of gpac@@gpac-v1.0.1-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 2341 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	2345	2345
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static void tx3g_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
2345.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=87
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	2475	2475
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2475.            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=1000025&projectid=19&pathid=88
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	2498	2498
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2498.                           memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=89
Status	New

The size of the buffer used by txtin_process_texml in GF_StyleRecord, at line 2435 of gpac@@gpac-v1.0.1-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 2435 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	2565	2565
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2565.
      memset(&styles[nb_styles], 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=90
Status	New

The size of the buffer used by txtin_process_texml in Marker, at line 2435 of gpac@@gpac-v1.0.1-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 Marker, at line 2435 of gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	2683	2683
Object	Marker	Marker

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method	static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2683.
      memset(&marks[nb_marks], 0, sizeof(Marker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=91
Status	New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 650 of gpac@@gpac-v1.0.1-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_hevc_set_parall_type passes to HEVCState, at line 650 of gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	657	657
Object	HEVCState	HEVCState

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method	static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

```
....
657.        memset(&hevc, 0, sizeof(HEVCState));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=92
Status	New

The size of the buffer used by gf_bifs_dec_proto_list in GF_FieldInfo, at line 994 of gpac@@gpac-v1.0.1-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 gf_bifs_dec_proto_list passes to GF_FieldInfo, at line 994 of gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c

Line	1096	1096
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Method GF_Err gf_bifs_dec_proto_list(GF_BifsDecoder * codec, GF_BitStream *bs, GF_List *proto_list)

```
....
1096.                   memset(&field, 0, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=93
Status New

The size of the buffer used by swf_get_matrix in GF_Matrix2D, at line 238 of gpac@@gpac-v1.0.1-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_get_matrix passes to GF_Matrix2D, at line 238 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	243	243
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static u32 swf_get_matrix(SWFReader *read, GF_Matrix2D *mat)

```
....
243.        memset(mat, 0, sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=94
Status New

The size of the buffer used by swf_get_colormatrix in GF_ColorMatrix, at line 290 of gpac@@gpac-v1.0.1-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_get_colormatrix passes to GF_ColorMatrix, at line 290 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	294	294
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static void swf_get_colormatrix(SWFReader *read, GF_ColorMatrix *cmat)

```
....
294.        memset(cmat, 0, sizeof(GF_ColorMatrix));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=95
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFPath, at line 360 of gpac@@gpac-v1.0.1-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 SWFPath, at line 360 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	365	365
Object	SWFPath	SWFPath

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
365.        memset(new_sr->path, 0, sizeof(SWFPath));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=96
Status	New

The size of the buffer used by swf_resort_path in SWFPath, at line 608 of gpac@@gpac-v1.0.1-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_resort_path passes to SWFPath, at line 608 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	737	737
Object	SWFPath	SWFPath

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static void swf_resort_path(SWFPath *a, SWFReader *read)

```
....
737.        memset(a, 0, sizeof(SWFPath));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=97
Status New

The size of the buffer used by swf_parse_shape_def in SWFShape, at line 878 of gpac@@gpac-v1.0.1-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_parse_shape_def passes to SWFShape, at line 878 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	890	890
Object	SWFShape	SWFShape

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_parse_shape_def(SWFReader *read, SWFFont *font, u32 revision)

```
....
890.        memset(&shape, 0, sizeof(SWFShape));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=98
Status New

The size of the buffer used by *swf_get_depth_entry in GF_Matrix2D, at line 1050 of gpac@@gpac-v1.0.1-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_get_depth_entry passes to GF_Matrix2D, at line 1050 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1065	1065
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static DispShape *swf_get_depth_entry(SWFReader *read, u32 Depth, Bool create)

```
....
1065.       memset(&tmp->mat, 0, sizeof(GF_Matrix2D));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=99
Status New

The size of the buffer used by *swf_get_depth_entry in GF_ColorMatrix, at line 1050 of gpac@@gpac-v1.0.1-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_get_depth_entry passes to GF_ColorMatrix, at line 1050 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1068	1068
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static DispShape *swf_get_depth_entry(SWFReader *read, u32 Depth, Bool create)

```
....
1068.       memset(&tmp->cmat, 0, sizeof(GF_ColorMatrix));
```

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=1000025&projectid=19&pathid=45
Status	New

The application performs an illegal operation in mp3_dmx_check_dur, in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-3291-TP.c, at line 111.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Line	148	148
Object	prev_sr	prev_sr

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=46
Status	New

The application performs an illegal operation in mp3_dmx_check_dur, in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-3291-TP.c, at line 111.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Line	151	151
Object	prev_sr	prev_sr

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Method static void mp3_dmx_check_dur(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
151.                    cur_dur /= prev_sr;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=47
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, 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 ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c	gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7812.             if (ctrn->ctso_multiplier) return
ctrn_s32_to_index(ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=48
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, 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 ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c	gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-11558-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7816.       if (ctrn->ctso_multiplier) return
ctrn_u32_to_index((u32)ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=49
Status	New

The application performs an illegal operation in isor_declare_track, in gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c. In line 79, the program attempts to divide by track_dur, 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 track_dur in isor_declare_track of gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c, at line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	883	883
Object	track_dur	track_dur

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
883.                    avgrate = (u64) (avgrate / track_dur);
```

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=1000025&projectid=19&pathid=287
Status	New

The buffer allocated by c in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-3523-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3523-TP.c
Line	313	330
Object	16	c

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=288
Status	New

The buffer allocated by c in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-3523-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3523-TP.c
Line	313	329
Object	16	c

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=289
Status	New

The buffer allocated by c in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-3523-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3523-TP.c
Line	313	331
Object	16	c

Code Snippet
File Name gpac@@gpac-v1.0.1-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];
```

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=1000025&projectid=19&pathid=1385
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	534	553
Object	continuous	continuous

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method GF_Err avidmx_process(GF_Filter *filter)

```
....
534.                    int continuous;
....
553.                    if (continuous)
```

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=1000025&projectid=19&pathid=1201
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 49 is not initialized when it is used by Pointer at gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c in line 49.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	211	211
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v1.0.1-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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1202
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 848 is not initialized when it is used by def_name at gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c in line 848.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	877	877
Object	null	def_name

Code Snippet
File Name gpac@@gpac-v1.0.1-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 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1203
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	270
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    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 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1204
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	270

Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

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

NULL Pointer Dereference\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1205
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	271
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
271.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CODECID, &PROP_UINT( codecid) );
```

NULL Pointer Dereference\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1206
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination

File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	271
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
271.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CODECID, &PROP_UINT( codecid) );
```

NULL Pointer Dereference\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1207
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	273
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
273.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_SAMPLE_RATE, &PROP_UINT( st->freq ) );
```

NULL Pointer Dereference\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1208
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	273
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
273.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_SAMPLE_RATE, &PROP_UINT( st->freq ) );
```

NULL Pointer Dereference\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1209
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	275
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    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 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1210
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	275
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
275.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_NUM_CHANNELS, &PROP_UINT( st->nb_channels ) );
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1211
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	280
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1212
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	280
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
280.                      gf_filter_pid_set_property(st->opid,
GF_PROP_PID_ID, &PROP_UINT( 2 + st->stream_num) );
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1213
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	281
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
281.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CLOCK_ID, &PROP_UINT( sync_id ) );
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1214
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	281
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
281.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_CLOCK_ID, &PROP_UINT( sync_id ) );
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1215
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	282
Object	null	opid

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
282.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DURATION, &PROP_FRAC64( dur ) );
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1216
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	282
Object	null	opid

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                        st = NULL;
....
282.                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DURATION, &PROP_FRAC64( dur ) );
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1217
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-	gpac@@gpac-v1.0.1-CVE-2023-4678-

	TP.c	TP.c
Line	252	284
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    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 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1218
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	284
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                        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 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1219
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	287
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
287.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_UNFRAMED, &PROP_BOOL( GF_TRUE ) );
```

NULL Pointer Dereference\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1220
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	287
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
287.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_UNFRAMED, &PROP_BOOL( GF_TRUE ) );
```

NULL Pointer Dereference\Path 21:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1221
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	294
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
294.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_TIMESCALE, &PROP_UINT(st->freq) );
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1222
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	294
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                          st = NULL;
....
294.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_TIMESCALE, &PROP_UINT(st->freq) );
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1223
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	308
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            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 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1224
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	308
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    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 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1225
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	291
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                            st = NULL;
....
291.                                    gf_filter_pid_set_property(st->opid,
GF_PROP_PID_AUDIO_FORMAT, &PROP_UINT(afmt) );
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1226
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	252	291
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
291.                                gf_filter_pid_set_property(st->opid,
GF_PROP_PID_AUDIO_FORMAT, &PROP_UINT(afmt) );
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1227
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Line	257	279
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
257.                        st = NULL;
....
279.                        gf_filter_pid_set_property(st->opid,
GF_PROP_PID_BITRATE, &PROP_UINT( brate ) );
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1228
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4678-	gpac@@gpac-v1.0.1-CVE-2023-4678-

	TP.c	TP.c
Line	252	279
Object	null	opid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
252.                    AVIAstream *st = NULL;
....
279.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_BITRATE, &PROP_UINT( brate ) );
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1229
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c in line 1243 is not initialized when it is used by have_dts at gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c
Line	1353	1119
Object	null	have_dts

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c
Method static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1353.                           add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name gpac@@gpac-v1.0.1-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 30:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1230
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c in line 1243 is not initialized when it is used by have_pts at gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c
Line	1353	1119
Object	null	have_pts

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4681-TP.c
Method static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1353.                           add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name gpac@@gpac-v1.0.1-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 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1231
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	1288	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v1.0.1-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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1232
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1233
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	1512	1512

Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v1.0.1-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 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1234
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c in line 1243 is not initialized when it is used by have_dts at gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c
Line	1353	1119
Object	null	have_dts

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c
Method static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1353.                           add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name gpac@@gpac-v1.0.1-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 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1235
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c in line 1243 is not initialized when it is used by have_pts at gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c
Line	1353	1119
Object	null	have_pts

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4721-TP.c
Method static void mpeg2ps_scan_file (mpeg2ps_t *ps)

```
....
1353.                           add_stream(ps, stream_id, substream, 0,
NULL);
```

File Name gpac@@gpac-v1.0.1-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 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1236
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v1.0.1-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 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1237
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	1288	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v1.0.1-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 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1238
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1239
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	1288	1327
Object	null	sgprivate

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1240
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c

Line	1271	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v1.0.1-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 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1241
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v1.0.1-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 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1242
Status New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by track at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	878
Object	null	track

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
878.         gf_isom_get_bitrate(read->mov, ch->track, stsd_idx,
&avg_rate, &max_rate, &buffer_size);
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1243
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	813
Object	null	pid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
813.        gf_filter_pid_set_property(ch->pid, GF_PROP_PID_CODECID,
&PROP_UINT(codec_id));
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1244
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	831
Object	null	pid

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
831.        gf_filter_pid_set_property(ch->pid, GF_PROP_PID_CONFIG_IDX,
&PROP_UINT(stsd_idx) );
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1245
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	897
Object	null	pid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
897.        gf_filter_pid_set_property(ch->pid,
GF_PROP_PID_ISOM_SUBTYPE, &PROP_UINT(m_subtype) );
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1246
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	954
Object	null	pid

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
954.              gf_filter_pid_set_property_str(ch->pid,
"codec_vendor", &PROP_UINT(udesc->vendor_code));
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1247
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	955
Object	null	pid

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
955.              gf_filter_pid_set_property_str(ch->pid,
"codec_version", &PROP_UINT(udesc->version));
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1248
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	956
Object	null	pid

Code Snippet

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c

Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
956.              gf_filter_pid_set_property_str(ch->pid,
"codec_revision", &PROP_UINT(udesc->revision));
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1249
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	957
Object	null	pid

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
957.              gf_filter_pid_set_property_str(ch->pid,
"compressor_name", &PROP_STRING(udesc->compressor_name));
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1250
Status	New

The variable declared in null at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 1003 is not initialized when it is used by pid at gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c in line 79.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	1136	958
Object	null	pid

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	GF_Err isor_declare_objects(ISOMReader *read)

```
....
1136.             isor_declare_track(read, NULL, i+1, stsd_idx,
streamtype, use_iod);
```

File Name	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method	static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
958.              gf_filter_pid_set_property_str(ch->pid,
"temporal_quality", &PROP_UINT(udesc->temporal_quality));
```

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=1000025&projectid=19&pathid=1318
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	249	249
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
249.                                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=1000025&projectid=19&pathid=1319
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	255	255
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
255.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1320
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	261	261
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
261.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1321
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	264	264
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
264.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1322
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	270	270
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
270.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1323
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	273	273
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
273.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1324
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	276	276
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
276.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1325
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	284	284
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
284.                        szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19

	&pathid=1326
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	287	287
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
287.                szLineConv[j] = 0;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1327
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c	gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Line	735	735
Object	alen	alen

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-0818-TP.c
Method static GF_Err txtin_process_srt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
735.                                    szLine[alen] = 0;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1328
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-	gpac@@gpac-v1.0.1-CVE-2023-1452-

	TP.c	TP.c
Line	249	249
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
249.                                    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=1000025&projectid=19&pathid=1329
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	255	255
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
255.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1330
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	261	261

Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
261.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1331
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	264	264
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
264.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1332
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	270	270
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c

Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
270.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1333
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	273	273
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
273.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1334
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	276	276
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
276.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1335
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	284	284
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
284.                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1336
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	287	287
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
287.                szLineConv[j] = 0;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1337
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c	gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Line	735	735
Object	alen	alen

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-1452-TP.c
Method static GF_Err txtin_process_srt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
735.                                szLine[alen] = 0;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1338
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-23144-TP.c	gpac@@gpac-v1.0.1-CVE-2023-23144-TP.c
Line	307	307
Object	orient	orient

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1339

Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	799	799
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
799.                            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=1000025&projectid=19&pathid=1340
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c	gpac@@gpac-v1.0.1-CVE-2023-41000-TP.c
Line	212	212
Object	count	count

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1341
Status	New

	Source	Destination

File	gpac@@gpac-v1.0.1-CVE-2023-42298-TP.c	gpac@@gpac-v1.0.1-CVE-2023-42298-TP.c
Line	307	307
Object	orient	orient

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1342
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1343
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	502	502

Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1344
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1345
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1346
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	536	536
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1347
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	3210	3210
Object	NbODs	NbODs

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Method	void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3210.                           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=1000025&projectid=19&pathid=1348
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1349
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19

	&pathid=1350
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1351
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1352
Status	New

	Source	Destination

File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	536	536
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1353
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1354
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1355
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1356
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1357
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	536	536
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1358
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	3210	3210
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Method void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3210.                          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=1000025&projectid=19&pathid=1359
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	3210	3210
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Method void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3210.                           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=1000025&projectid=19&pathid=1360
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	632	632
Object	len	len

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
632.                                buffer[len] = 0;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1361
Status	New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	636	636
Object	l1	l1

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
636.                                    tx3g_config_sdp[l1] = 0;
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1362
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Line	249	249
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
249.                                    szLineConv[j] = 0xc0 | ( (szLine[i]
>> 6) & 0x3 );
```

Unchecked Array Index\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1363
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c

Line	255	255
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
255.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1364
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Line	261	261
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
261.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1365
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Line	264	264
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
264.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 49:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1366
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Line	270	270
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
270.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 50:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1367
Status New

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c	gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Line	273	273
Object	j	j

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2024-0321-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
273.                                    szLineConv[j] = szLine[i];
```

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=1000025&projectid=19&pathid=1159
Status	New

The naludmx_process method calls the sprintf function, at line 2087 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	3027	3027
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3027.             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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1160
Status	New

The id3dmx_flush method calls the sprintf function, at line 215 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-3291-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Line	311	311
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Method void id3dmx_flush(GF_Filter *filter, u8 *id3_buf, u32 id3_buf_size, GF_FilterPid *audio_pid, GF_FilterPid **video_pid_p)

```
....
311.                    sprintf(szTag, "tag_%s", gf_4cc_to_str(ftag));
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1161
Status New

The gf_bifs_dec_proto_list method calls the sprintf function, at line 994 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	1027	1027
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-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 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1162
Status New

The gf_bifs_dec_proto_list method calls the sprintf function, at line 994 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-37767-TP.c	gpac@@gpac-v1.0.1-CVE-2023-37767-TP.c
Line	1051	1051
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-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 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1163
Status New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2667	2667
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2667.                           sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19

	&pathid=1164
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2669	2669
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2669.                           sprintf(svgFileName, "%s.svg", load->svgOutFile);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1165
Status	New

The swf_def_sound method calls the sprintf function, at line 1790 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1820	1820
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_sound(SWFReader *read)

```
....
1820.              sprintf(szName, "swf_sound_%d.mp3", snd->ID);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1166
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1962	1962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                   sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1167
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1964	1964
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1964.                   sprintf(szName, "swf_soundstream_%d.mp3", read-
>current_sprite_id);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1168
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2079	2079
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2079.             sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1169
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2081	2081
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2081.             sprintf(szName, "swf_jpeg_%d.jpg", ID);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1170
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2155	2155
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2155.                   sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1171
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2157	2157
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2157.                    sprintf(szName, "swf_png_%d.png", ID);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1172
Status	New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v1.0.1-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1173
Status	New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4683-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4683-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v1.0.1-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 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1174
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2667	2667
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method	GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2667.                           sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1175
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2669	2669

Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2669.                           sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1176
Status	New

The swf_def_sound method calls the sprintf function, at line 1790 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1820	1820
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_sound(SWFReader *read)

```
....
1820.             sprintf(szName, "swf_sound_%d.mp3", snd->ID);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1177
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c

Line	1962	1962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                   sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1178
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1964	1964
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1964.                   sprintf(szName, "swf_soundstream_%d.mp3", read-
>current_sprite_id);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1179
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2079	2079
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2079.            sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1180
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2081	2081
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2081.            sprintf(szName, "swf_jpeg_%d.jpg", ID);
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1181
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2155	2155
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2155.                    sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1182
Status New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2157	2157
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2157.                    sprintf(szName, "swf_png_%d.png", ID);
```

Unchecked Return Value\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1183
Status New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2667	2667
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2667.                           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=1000025&projectid=19&pathid=1184
Status New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2669	2669
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2669.                           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=1000025&projectid=19

	&pathid=1185
Status	New

The swf_def_sound method calls the sprintf function, at line 1790 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1820	1820
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_sound(SWFReader *read)

```
....
1820.             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=1000025&projectid=19&pathid=1186
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1962	1962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                   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=1000025&projectid=19&pathid=1187
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1964	1964
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1964.                    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=1000025&projectid=19&pathid=1188
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2079	2079
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2079.             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=1000025&projectid=19&pathid=1189
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2081	2081
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2081.             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=1000025&projectid=19&pathid=1190
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2155	2155
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2155.                    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=1000025&projectid=19&pathid=1191
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2157	2157
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2157.                    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=1000025&projectid=19&pathid=1192
Status	New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v1.0.1-CVE-2023-4756-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-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v1.0.1-CVE-2023-4756-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 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1193
Status	New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v1.0.1-CVE-2023-4756-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-v1.0.1-CVE-2023-4756-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4756-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4756-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 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1194
Status	New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v1.0.1-CVE-2023-4778-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-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4778-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 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1195
Status	New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v1.0.1-CVE-2023-4778-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-v1.0.1-CVE-2023-4778-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4778-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4778-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 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1196
Status	New

The isor_declare_track method calls the sprintf function, at line 79 of gpac@@gpac-v1.0.1-CVE-2023-5595-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-v1.0.1-CVE-2023-5595-TP.c	gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Line	372	372

Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-5595-TP.c
Method static void isor_declare_track(ISOMReader *read, ISOMChannel *ch, u32 track, u32 stsd_idx, u32 streamtype, Bool use_iod)

```
....
372.                    sprintf(szPName, "%c%d", szST[0], esid);
```

Unchecked Return Value\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1197
Status New

The dump_mpeg2_ts method calls the sprintf function, at line 4120 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4152	4152
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4152.                   sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Unchecked Return Value\Path 40:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1198
Status New

The dump_mpeg2_ts method calls the sprintf function, at line 4120 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-	gpac@@gpac-v2.0.0-CVE-2020-23932-

	FP.c	FP.c
Line	4189	4189
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4189.             sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

Improper Resource Access Authorization

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

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Improper Resource Access Authorization\Path 1:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1956
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4347	4347
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4347.       fprintf(stderr, "Downloading %s\n", mpd_src);
```

Improper Resource Access Authorization\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1957
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4440	4440
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4440.                           fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1958
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4468	4468
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4468.                               fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1959
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Line	3933	3933
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3933.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1960
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3938	3938
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3938.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1961
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3946	3946
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3946.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1962
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3952	3952
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3952.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1963
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3957	3957
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3957.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1964
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3962	3962
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3962.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1965
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3986	3986
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3986.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1966
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	3994	3994
Object	fprintf	fprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3994.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1967
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4002	4002
Object	fprintf	fprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c

Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4002.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1968
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4059	4059
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4059.                          fprintf(dumper->timestamps_info_file,
"%u\t%d\t", pck->stream->pes_start_packet_number, pck->stream->pid);
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1969
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4060	4060
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4060.                          if (interpolated_pcr_value)
fprintf(dumper->timestamps_info_file, "%f",
interpolated_pcr_value/(300.0 * 90000));
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1970
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4061	4061
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4061.                          fprintf(dumper->timestamps_info_file,
"\t");
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1971
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4062	4062
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4062.                          if (pck->DTS) fprintf(dumper-
>timestamps_info_file, "%f", (pck->DTS / 90000.0));
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1972
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4063	4063
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4063.                          fprintf(dumper->timestamps_info_file,
"\t%f\t%d\t%d", pck->PTS / 90000.0, (pck->flags & GF_M2TS_PES_PCK_RAP) ?
1 : 0, (pck->flags & GF_M2TS_PES_PCK_DISCONTINUITY) ? 1 : 0);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1973
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4067	4067
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4067.                                   fprintf(dumper-
>timestamps_info_file, "\t%f\n", diff);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1974
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4072	4072
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4072.                                   fprintf(dumper-
>timestamps_info_file, "\t\n");
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1975
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4086	4086
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4086.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\t%f\t\t\t\t%d\n", pck->stream->program-
>last_pcr_value_pck_number, pck->stream->pid, pck->PTS / (300*90000.0),
(pck->flags & GF_M2TS_PES_PCK_DISCONTINUITY) ? 1 : 0);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1976
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4131	4131
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4131.             fprintf(stderr, "No program number nor output filename
specified. No timestamp file will be generated.");
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1977
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4181	4181
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4181.             fprintf(stderr, "No program number specified,
defaulting to first program\n");
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1978
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4185	4185
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4185.             fprintf(stderr, "No program number nor output filename
specified. No timestamp file will be generated\n");
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1979
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4195	4195
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4195.             fprintf(dumper.timestamps_info_file,
"PCK#\tPID\tPCR\tDTS\tPTS\tRAP\tDiscontinuity\tDTS-PCR Diff\n");
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1980
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4238	4238
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void get_file_callback(void *usr_cbk, GF_NETIO_Parameter *parameter)

```
....
4238.                    fprintf(stderr, "download %02d %% at %05d
kpbs\r", (u32) max, bps*8/1000);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1981
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4263	4263
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method static void revert_cache_file(char *item_path)

```
....
4263.              fprintf(stderr, "%s is not a gpac cache file\n",
item_path);
```

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=1000025&projectid=19&pathid=1299
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 2087 of gpac@@gpac-v1.0.1-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 2087 of gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c	gpac@@gpac-v1.0.1-CVE-2023-2839-TP.c
Line	3027	3027
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-v1.0.1-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3027.              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 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1300
Status	New

The size of the buffer used by id3dmx_flush in "tag_%s", at line 215 of gpac@@gpac-v1.0.1-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 id3dmx_flush passes to "tag_%s", at line 215 of gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Line	311	311
Object	"tag_%s"	"tag_%s"

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-3291-TP.c
Method	void id3dmx_flush(GF_Filter *filter, u8 *id3_buf, u32 id3_buf_size, GF_FilterPid *audio_pid, GF_FilterPid **video_pid_p)

```
....
311.                    sprintf(szTag, "tag_%s", gf_4cc_to_str(ftag));
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1301
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s%c%s.svg", at line 2622 of gpac@@gpac-v1.0.1-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 2622 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2667	2667
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method	GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2667.                        sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1302
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2622 of gpac@@gpac-v1.0.1-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 2622 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c

Line	2669	2669
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2669.                          sprintf(svgFileName, "%s.svg", load->svgOutFile);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1303
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1922 of gpac@@gpac-v1.0.1-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 1922 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	1962	1962
Object	"%s/swf_soundstream_%d.mp3"	"%s/swf_soundstream_%d.mp3"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                   sprintf(szName, "%s/swf_soundstream_%d.mp3", read->localPath, read->current_sprite_id);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1304
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_jpeg_%d.jpg", at line 2054 of gpac@@gpac-v1.0.1-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 2054 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2079	2079
Object	"%s/swf_jpeg_%d.jpg"	"%s/swf_jpeg_%d.jpg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2079.             sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Potential Precision Problem\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1305
Status New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_png_%d.png", at line 2054 of gpac@@gpac-v1.0.1-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 2054 of gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c	gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Line	2155	2155
Object	"%s/swf_png_%d.png"	"%s/swf_png_%d.png"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-46426-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2155.                   sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Potential Precision Problem\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1306
Status New

The size of the buffer used by gf_sm_load_init_swf in "%s%c%s.svg", at line 2622 of gpac@@gpac-v1.0.1-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 2622 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2667	2667
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2667.                        sprintf(svgFileName, "%s%c%s.svg", load->localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Potential Precision Problem\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1307
Status New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2622 of gpac@@gpac-v1.0.1-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 2622 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2669	2669
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2669.                        sprintf(svgFileName, "%s.svg", load->svgOutFile);
```

Potential Precision Problem\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19

	&pathid=1308
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1922 of gpac@@gpac-v1.0.1-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 1922 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	1962	1962
Object	"%s/swf_soundstream_%d.mp3"	"%s/swf_soundstream_%d.mp3"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                   sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1309
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_jpeg_%d.jpg", at line 2054 of gpac@@gpac-v1.0.1-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 2054 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2079	2079
Object	"%s/swf_jpeg_%d.jpg"	"%s/swf_jpeg_%d.jpg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2079.               sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1310
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_png_%d.png", at line 2054 of gpac@@gpac-v1.0.1-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 2054 of gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Line	2155	2155
Object	"%s/swf_png_%d.png"	"%s/swf_png_%d.png"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4720-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2155.                    sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1311
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s%c%s.svg", at line 2622 of gpac@@gpac-v1.0.1-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 2622 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2667	2667
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2667.                          sprintf(svgFileName, "%s%c%s.svg", load-
>localPath, GF_PATH_SEPARATOR, load->svgOutFile);
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1312
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2622 of gpac@@gpac-v1.0.1-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 2622 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2669	2669
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method GF_Err gf_sm_load_init_swf(GF_SceneLoader *load)

```
....
2669.                          sprintf(svgFileName, "%s.svg", load-
>svgOutFile);
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1313
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1922 of gpac@@gpac-v1.0.1-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 1922 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	1962	1962
Object	"%s/swf_soundstream_%d.mp3"	"%s/swf_soundstream_%d.mp3"

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method	static GF_Err swf_soundstream_hdr(SWFReader *read)

```
....
1962.                    sprintf(szName, "%s/swf_soundstream_%d.mp3",
read->localPath, read->current_sprite_id);
```

Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1314
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_jpeg_%d.jpg", at line 2054 of gpac@@gpac-v1.0.1-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 2054 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Line	2079	2079
Object	"%s/swf_jpeg_%d.jpg"	"%s/swf_jpeg_%d.jpg"

Code Snippet	
File Name	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method	static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2079.            sprintf(szName, "%s/swf_jpeg_%d.jpg", read->localPath,
ID);
```

Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1315
Status	New

The size of the buffer used by swf_def_bits_jpeg in "%s/swf_png_%d.png", at line 2054 of gpac@@gpac-v1.0.1-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 2054 of gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c	gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c

Line	2155	2155
Object	"%s/swf_png_%d.png"	"%s/swf_png_%d.png"

Code Snippet
File Name gpac@@gpac-v1.0.1-CVE-2023-4754-TP.c
Method static GF_Err swf_def_bits_jpeg(SWFReader *read, u32 version)

```
....
2155.                    sprintf(szName, "%s/swf_png_%d.png", read-
>localPath, ID);
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1316
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_%d.raw", at line 4120 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_mpeg2_ts passes to "%s_%d.raw", at line 4120 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4152	4152
Object	"%s_%d.raw"	"%s_%d.raw"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4152.                    sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000025&projectid=19&pathid=1317
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_prog_%d_timestamps.txt", at line 4120 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_mpeg2_ts passes to "%s_prog_%d_timestamps.txt", at line 4120 of gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c	gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Line	4189	4189
Object	"%s_prog_%d_timestamps.txt"	"%s_prog_%d_timestamps.txt"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2020-23932-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4189.             sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

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=1000025&projectid=19&pathid=1199
Status	New

The buffer allocated by <= in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47659-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Line	116	116
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v1.0.1-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=1000025&projectid=19&pathid=1200
Status	New

The buffer allocated by <= in gpac@@gpac-v1.0.1-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-v1.0.1-CVE-2022-47659-TP.c	gpac@@gpac-v1.0.1-CVE-2022-47659-TP.c
Line	119	119
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v1.0.1-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

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));

      return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
      int total = Integer.parseInt(req.getParameter("total"));
      int count = Integer.parseInt(req.getParameter("count"));
```

```
	if (count > 0)
		return total / count;
	else
		return 0;
}
```

Buffer Overflow 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

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025