vul_files_19 Scan Report

Project Name	vul_files_19
Scan Start	Tuesday, January 7, 2025 2:37:48 PM
Preset	Checkmarx Default
Scan Time	01h:24m:14s
Lines Of Code Scanned	297790
Files Scanned	60
Report Creation Time	Tuesday, January 7, 2025 4:09:08 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	5/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

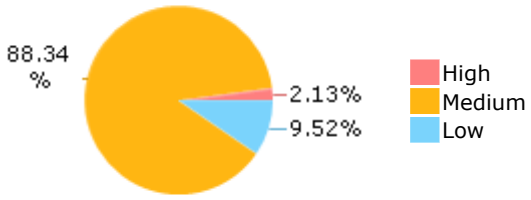
Results Limit

Results limit per query was set to 50

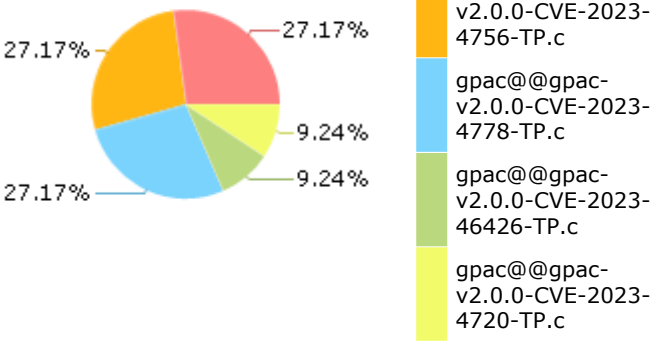
Selected Queries

Selected queries are listed in Result Summary

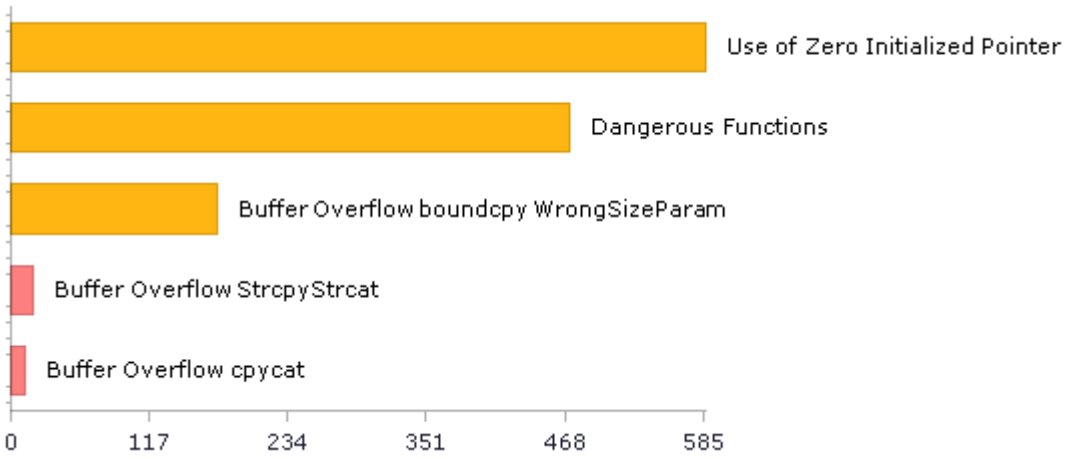
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	276	221
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	472	472
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

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

Scan Summary - OWASP Top 10 2013

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

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS)	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	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	472	472
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	0	0
PCI DSS (3.2) - 6.5.2 - Buffer overflows	207	184
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

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

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	636	77
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	75	54
SI-11 Error Handling (P2)*	41	41
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	3	1

***** 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

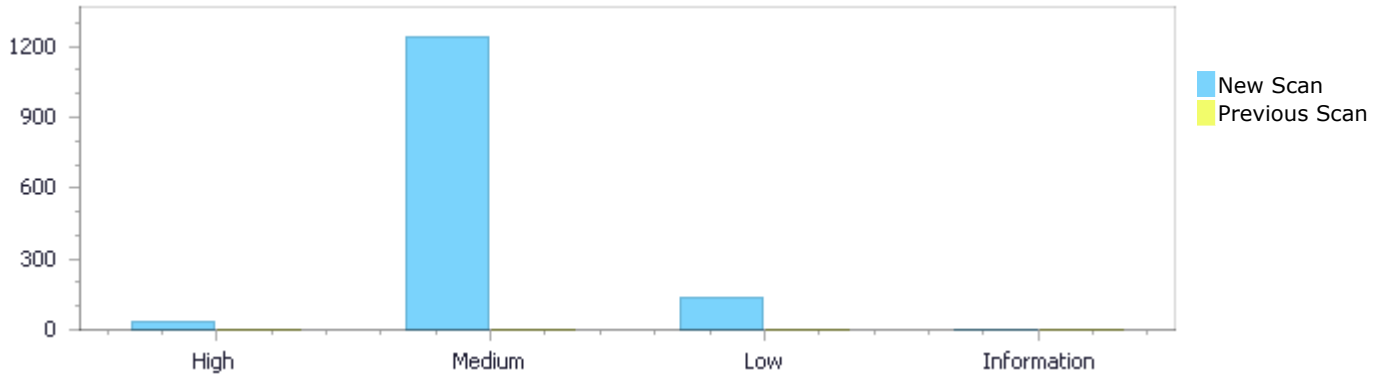
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, 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	30	1,243	134	0	1,407
Recurrent Issues	0	0	0	0	0
Total	30	1,243	134	0	1,407
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	30	1,243	134	0	1,407
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	30	1,243	134	0	1,407

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	18	High
Buffer Overflow cpycat	12	High
Use of Zero Initialized Pointer	587	Medium
Dangerous Functions	472	Medium
Buffer Overflow boundcpy WrongSizeParam	174	Medium

Divide By Zero	6	Medium
Buffer Overflow Loops	3	Medium
Use of Uninitialized Variable	1	Medium
NULL Pointer Dereference	48	Low
Unchecked Return Value	41	Low
Unchecked Array Index	24	Low
Potential Precision Problem	21	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	235
gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	235
gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	235
gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	76
gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	76
gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	63
gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	63
gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	63
gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	52
gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c	33

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=1020036&projectid=20029&pathid=13
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 2:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=14
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=15
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=16
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=17
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=18
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c

Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=19
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=20
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=21
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=22
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=23
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v2.0.0-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-v2.0.0-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 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=24
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 13:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=25
Status New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v2.0.0-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 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=26
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v2.0.0-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 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=27
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v2.0.0-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 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=28
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v2.0.0-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 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=29
Status	New

The size of the buffer used by *gf_bt_peek_node in defID, at line 1578 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-	gpac@@gpac-v2.0.0-CVE-2023-4778-

	TP.c	TP.c
Line	1578	1600
Object	defID	defID

Code Snippet
File Name gpac@@gpac-v2.0.0-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 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=30
Status	New

The size of the buffer used by *gf_bt_peek_node in nName, at line 1578 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	1578	1600
Object	defID	nName

Code Snippet
File Name gpac@@gpac-v2.0.0-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 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=1020036&projectid=20029&pathid=1
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=2
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c

Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=3
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=4
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=5
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=6
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=7
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=8
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	377	1983
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=9
Status New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=10
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1950
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=11
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=12
Status	New

The size of the buffer used by *gf_bt_parse_route in parser, at line 1927 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	377	1983
Object	Address	parser

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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-v2.0.0-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));
```

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=1020036&projectid=20029&pathid=821
Status	New

The variable declared in output at gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c in line 839 is not initialized when it is used by pck at gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c in line 839.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	843	855
Object	output	pck

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method	static GF_Err av1dmx_parse_flush_sample(GF_Filter *filter, GF_AV1DmxCtx *ctx)

```
....
843.        u8 *output = NULL;
....
855.        pck = gf_filter_pck_new_alloc(ctx->opid, pck_size, &output);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=822
Status	New

The variable declared in dsi at gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c in line 519 is not initialized when it is used by pck at gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c in line 839.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	531	855
Object	dsi	pck

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c

Method static void av1dmx_check_pid(GF_Filter *filter, GF_AV1DmxCtx *ctx)

```
....
531.        dsi = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c

Method static GF_Err av1dmx_parse_flush_sample(GF_Filter *filter, GF_AV1DmxCtx *ctx)

```
....
855.        pck = gf_filter_pck_new_alloc(ctx->opid, pck_size, &output);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=823
Status	New

The variable declared in vp_cfg at gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c in line 148 is not initialized when it is used by pck at gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c in line 839.

	Source	Destination

File	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	162	855
Object	vp_cfg	pck

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method GF_Err av1dmx_check_format(GF_Filter *filter, GF_AV1DmxCtx *ctx, GF_BitStream *bs, u32 *last_obu_end)

```
....
162.        ctx->vp_cfg = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method static GF_Err av1dmx_parse_flush_sample(GF_Filter *filter, GF_AV1DmxCtx *ctx)

```
....
855.        pck = gf_filter_pck_new_alloc(ctx->opid, pck_size, &output);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=824
Status	New

The variable declared in avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 412 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 412.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	417	540
Object	avc_state	avc_state

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

```
....
417.        AVCState *avc_state = NULL;
....
540.                    nal_type = avc_state->last_nal_type_parsed;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=825
Status	New

The variable declared in pa at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 739 is not initialized when it is used by pa at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 739.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	747	758
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_add_param_nalu(GF_List *param_list, GF_NALUFFParam *sl, u8 nal_type)

```
....
747.                pa = NULL;
....
758.        gf_list_add(pa->nalus, sl);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=826
Status	New

The variable declared in pa at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 739 is not initialized when it is used by pa at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 739.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	741	758
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_add_param_nalu(GF_List *param_list, GF_NALUFFParam *sl, u8 nal_type)

```
....
741.        GF_NALUFFParamArray *pa = NULL;
....
758.        gf_list_add(pa->nalus, sl);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=827
Status	New

The variable declared in _buf at gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c in line 223 is not initialized when it is used by _buf at gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c in line 223.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	227	263
Object	_buf	_buf

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
227.        char *_buf=NULL;
....
263.                    _buf = gf_realloc(_buf, fsize+3);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=828
Status	New

The variable declared in offset_table at gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c in line 1418 is not initialized when it is used by offset_table at gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c in line 1418.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1423	1489
Object	offset_table	offset_table

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=829
Status	New

The variable declared in st at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by st at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	287
Object	st	st

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=830
Status	New

The variable declared in st at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by st at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c

Line	258	287
Object	st	st

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=831
Status	New

The variable declared in offset_table at gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c in line 1418 is not initialized when it is used by offset_table at gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c in line 1418.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1423	1489
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v2.0.0-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 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=832
Status	New

The variable declared in offset_table at gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c in line 1418 is not initialized when it is used by offset_table at gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c in line 1418.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1423	1489
Object	offset_table	offset_table

Code Snippet
File Name gpac@@gpac-v2.0.0-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 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=833
Status	New

The variable declared in key_info at gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c in line 191 is not initialized when it is used by key_info at gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c in line 191.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	198	219
Object	key_info	key_info

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method static void isor_update_cenc_info(ISOMChannel *ch, Bool for_item)

```
....
198.        u8 *key_info = NULL;
....
219.                    item_mkey = key_info[0];
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=834
Status	New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err stsc_box_read(GF_Box *s, GF_BitStream *bs)

```
....
5361.        ptr->entries = NULL;
....
5379.                if (i) ptr->entries[i-1].nextChunk = ptr-
>entries[i].firstChunk;
```

Use of Zero Initialized Pointer\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=835
Status New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err stsc_box_read(GF_Box *s, GF_BitStream *bs)

```
....
5361.        ptr->entries = NULL;
....
5379.                if (i) ptr->entries[i-1].nextChunk = ptr-
>entries[i].firstChunk;
```

Use of Zero Initialized Pointer\Path 16:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=836
Status	New

The variable declared in in_pck at gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c in line 448 is not initialized when it is used by src_pck at gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c in line 448.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Line	488	745
Object	in_pck	src_pck

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Method GF_Err mhas_dmx_process(GF_Filter *filter)

```
....
488.              in_pck = NULL;
....
745.                                  ctx->src_pck = in_pck;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=837
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2642
Object	Pointer	avc_state

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.        *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
2642.                    ctx->avc_state->s_info.poc = ctx->last_poc;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=838
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	2642
Object	Pointer	avc_state

Code Snippet

File Name	gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
2642.                    ctx->avc_state->s_info.poc = ctx->last_poc;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=839
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	2642
Object	Pointer	avc_state

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2642.                   ctx->avc_state->s_info.poc = ctx->last_poc;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=840
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	1832
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method	static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1832.                   list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=841
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	1832
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1832.                   list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=842
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	1832
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1832.                   list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=843
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Line	1294	1848
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1848.                   list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=844
Status New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	1848
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1848.                    list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=845
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	1848
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1848.                    list = ctx->vps;
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=846
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	1880
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1880.                   list = ctx->sps_ext;
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=847
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	1880
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1880.                   list = ctx->sps_ext;
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=848
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	1880
Object	Pointer	list

Code Snippet

File Name	gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1880.                   list = ctx->sps_ext;
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=849
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2067.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2079
Object	Pointer	first_pck_in_au

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2079.            ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=850
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2067.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Line	1444	2079
Object	Pointer	first_pck_in_au

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2079.            ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=851
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by first_pck_in_au at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2067.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	2079
Object	Pointer	first_pck_in_au

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2079.              ctx->first_pck_in_au = dst_pck;
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=852
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	1838
Object	Pointer	list

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name	gpac@@gpac-v2.0.0-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)

```
....
1838.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=853
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	1838
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1838.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=854
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	1854
Object	Pointer	list

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
1444.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1854.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=855
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	1854
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1854.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=856
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 970 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1103	1875
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1103.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1875.                   list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=857
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311 is not initialized when it is used by list at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1819.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1444	1875
Object	Pointer	list

Code Snippet

File Name gpac@@gpac-v2.0.0-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)

```
....
1444.        *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1875.                    list = ctx->pps;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=858
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2533
Object	Pointer	avc_state

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.        *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2533.                          GF_LOG(ctx->avc_state->sps[0].profile_idc
? GF_LOG_WARNING : GF_LOG_ERROR, GF_LOG_MEDIA, ("[%s] Error parsing
Sequence Param Set\n", ctx->log_name));
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=859
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2532
Object	Pointer	avc_state

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2532.                   if (ctx->avc_state->sps[0].profile_idc) {
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=860
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2530
Object	Pointer	avc_state

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2530.             ps_idx = ctx->avc_state->last_ps_idx;
```

Use of Zero Initialized Pointer\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=861
Status New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2542
Object	Pointer	avc_state

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2542.            ps_idx = ctx->avc_state->last_ps_idx;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=862
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2552
Object	Pointer	avc_state

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2552.            ps_idx = ctx->avc_state->last_ps_idx;
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=863
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 2510.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	2644
Object	Pointer	avc_state

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
2644.          if (ctx->avc_state->s_info.sps) {
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=864
Status	New

The variable declared in Pointer at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1139 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 1311.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1294	1385
Object	Pointer	avc_state

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method static void naludmx_create_vvc_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_vvc_base)

```
....
1294.       *dsi = *dsi_enh = NULL;
```

File Name gpac@@gpac-v2.0.0-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)

```
....
1385.                               DeltaTfiDivisorIdx = 1 + (1 - ctx-
>avc_state->s_info.field_pic_flag);
```

Use of Zero Initialized Pointer\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=865
Status New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375 is not initialized when it is used by ActiveQP at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	383	395
Object	global_qp	ActiveQP

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c

Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
383.             codec->scenegraph->global_qp = NULL;
....
395.        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=1020036&projectid=20029&pathid=866
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375 is not initialized when it is used by ActiveQP at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	385	395
Object	ActiveQP	ActiveQP

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

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

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=867
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375 is not initialized when it is used by global_qp at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	383	393
Object	global_qp	global_qp

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

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

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=868
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375 is not initialized when it is used by global_qp at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 375.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	385	393
Object	ActiveQP	global_qp

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecGlobalQuantizer(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
385.        codec->ActiveQP = NULL;
....
393.        codec->scenegraph->global_qp = node;
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=869
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c in line 399.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	178	433
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-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 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=870
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c in line 399.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	177	433
Object	ActiveQP	new_node

Code Snippet

File Name gpac@@gpac-v2.0.0-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-v2.0.0-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;
```

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=1020036&projectid=20029&pathid=214
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2023-0760-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-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

```
....
681.        memcpy(ptr->nameURN, tmpName, i + 1);
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=215
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2023-0760-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-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

```
....
694.              memcpy(ptr->location, tmpName + i + 1, (to_read - i -
1));
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=216
Status	New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2023-0760-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-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err elng_box_read(GF_Box *s, GF_BitStream *bs)

```
....
3428.                   memcpy(str, ptr->extended_language, (u32) ptr-
>size);
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=217
Status	New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2023-0760-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-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	8089	8089
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c

Method	GF_Err udta_on_child_box(GF_Box *s, GF_Box *a, Bool is_rem)

```
....
8089.                    memcpy(map->uuid, ((GF_UUIDBox *)a)->uuid, 16);
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=218
Status	New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2023-0760-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-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method	static void *sgpd_parse_entry(u32 grouping_type, GF_BitStream *bs, s32 bytes_in_box, u32 entry_size, u32 *total_bytes)

```
....
9777.                    memcpy(ptr->key_info+4, kid, 16);
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=219
Status	New

The dangerous function, memcpy, was found in use at line 263 in gpac@@gpac-v2.0.0-CVE-2023-0817-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-v2.0.0-CVE-2023-0817-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Line	319	319
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c

Method	static void mhas_dmx_check_pid(GF_Filter *filter, GF_MHASDmxCtx *ctx, u32 PL, u32 sample_rate, u32 frame_len, s32 CICPspeakerLayoutIdx, s32 numSpeakers, u8 *dsi, u32 dsi_size)

```
....
319.                memcpy(data+5, dsi, dsi_size);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=220
Status	New

The dangerous function, memcpy, was found in use at line 448 in gpac@@gpac-v2.0.0-CVE-2023-0817-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-v2.0.0-CVE-2023-0817-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Line	509	509
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Method	GF_Err mhas_dmx_process(GF_Filter *filter)

```
....
509.                memcpy(ctx->mhas_buffer + ctx->mhas_buffer_size, data,
pck_size);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=221
Status	New

The dangerous function, memcpy, was found in use at line 448 in gpac@@gpac-v2.0.0-CVE-2023-0817-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-v2.0.0-CVE-2023-0817-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Line	714	714
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0817-TP.c
Method GF_Err mhas_dmx_process(GF_Filter *filter)

```
....
714.                    memcpy(output, start + au_start, au_size);
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=222
Status	New

The dangerous function, memcpy, was found in use at line 550 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-0866-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Line	605	605
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=223
Status	New

The dangerous function, memcpy, was found in use at line 550 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-0866-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Line	646	646
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=224
Status New

The dangerous function, memcpy, was found in use at line 550 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-0866-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Line	659	659
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=225
Status New

The dangerous function, memcpy, was found in use at line 550 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-0866-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Line	817	817
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=226
Status	New

The dangerous function, memcpy, was found in use at line 839 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	864	864
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method static GF_Err av1dmx_parse_flush_sample(GF_Filter *filter, GF_AV1DmxCtx *ctx)

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

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=227
Status	New

The dangerous function, memcpy, was found in use at line 1037 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	1099	1099
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

```
....
1099.                    memcpy(ctx->buffer+ctx->buf_size, data,
pck_size);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=228
Status	New

The dangerous function, memcpy, was found in use at line 1037 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	1133	1133
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

```
....
1133.                    memcpy(ctx->buffer+ctx->buf_size, data,
pck_size);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=229
Status	New

The dangerous function, memcpy, was found in use at line 1037 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-1449-TP.c	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Line	1151	1151
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-1449-TP.c
Method	GF_Err av1dmx_process(GF_Filter *filter)

```
....
1151.       memcpy(ctx->buffer+ctx->buf_size, data, pck_size);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=230
Status	New

The dangerous function, memcpy, was found in use at line 1139 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1223	1223
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method	static void naludmx_create_vvc_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_vvc_base)

```
....
1223.                               memcpy(cfg->general_constraint_info,
vps->ptl[0].gci, cfg->num_constraint_info);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=231
Status	New

The dangerous function, memcpy, was found in use at line 1819 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Line	1917	1917
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
1917.             memcpy(sl->data, data, size);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=232
Status	New

The dangerous function, memcpy, was found in use at line 1819 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	1932	1932
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
1932.       memcpy(sl->data, data, size);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=233
Status	New

The dangerous function, memcpy, was found in use at line 2128 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-	gpac@@gpac-v2.0.0-CVE-2023-2839-

	TP.c	TP.c
Line	2138	2138
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_push_prefix(GF_NALUDmxCtx *ctx, u8 *data, u32 size, Bool avc_sei_rewrite)

```
....
2138.       memcpy(ctx->sei_buffer + ctx->sei_buffer_size + ctx-
>nal_length, data, size);
```

Dangerous Functions\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=234
Status New

The dangerous function, memcpy, was found in use at line 2330 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	2476	2476
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static s32 naludmx_parse_nal_vvc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

```
....
2476.                   memcpy(ctx->init_aud, data, 3);
```

Dangerous Functions\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=235
Status New

The dangerous function, memcpy, was found in use at line 2510 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	2581	2581
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
2581.                    memcpy(ctx->init_aud, data, 2);
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=236
Status	New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	2843	2843
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2843.              memcpy(ctx->nal_store + ctx->nal_store_size, data,
sizeof(char)*pck_size);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=237
Status	New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3279	3279
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3279.                                   memcpy(ctx->svc_prefix_buffer,
start+sc_size, ctx->svc_prefix_buffer_size);
```

Dangerous Functions\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=238
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3484	3484
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3484.                    memcpy(pck_data + ctx->nal_length , ctx-
>init_aud, audelim_size);
```

Dangerous Functions\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=239
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3493	3493
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3493.                    memcpy(pck_data, ctx->sei_buffer, ctx-
>sei_buffer_size);
```

Dangerous Functions\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=240
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3502	3502
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3502.                    memcpy(pck_data + ctx->nal_length, ctx-
>svc_prefix_buffer, ctx->svc_prefix_buffer_size);
```

Dangerous Functions\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=241
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3520	3520
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3520.             memcpy(pck_data, nal_data, (size_t) nal_size);
```

Dangerous Functions\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=242
Status New

The dangerous function, memcpy, was found in use at line 223 in gpac@@gpac-v2.0.0-CVE-2023-3291-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-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	310	310
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
310.                                                memcpy(out_buffer,
sep_desc+1, pic_size);
```

Dangerous Functions\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=243
Status New

The dangerous function, memcpy, was found in use at line 490 in gpac@@gpac-v2.0.0-CVE-2023-3291-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-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	543	543
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Method GF_Err mp3_dmx_process(GF_Filter *filter)

```
....
543.                memcpy(ctx->mp3_buffer + ctx->mp3_buffer_size, data,
pck_size);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=244
Status	New

The dangerous function, memcpy, was found in use at line 490 in gpac@@gpac-v2.0.0-CVE-2023-3291-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-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	585	585
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Method GF_Err mp3_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=245
Status	New

The dangerous function, memcpy, was found in use at line 490 in gpac@@gpac-v2.0.0-CVE-2023-3291-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-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	598	598
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Method GF_Err mp3_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=246
Status New

The dangerous function, memcpy, was found in use at line 490 in gpac@@gpac-v2.0.0-CVE-2023-3291-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-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	662	662
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Method GF_Err mp3_dmx_process(GF_Filter *filter)

```
....
662.                    memcpy(output, sync, size);
```

Dangerous Functions\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=247
Status New

The dangerous function, memcpy, was found in use at line 555 in gpac@@gpac-v2.0.0-CVE-2023-3523-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-v2.0.0-CVE-2023-3523-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3523-TP.c
Line	635	635
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3523-TP.c
Method GF_Err vobsub_packetize_subpicture(FILE *fsub, u64 pts, u8 *data, u32 dataSize)

```
....
635.                memcpy(p, data, dataLen);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=248
Status	New

The dangerous function, memcpy, was found in use at line 59 in gpac@@gpac-v2.0.0-CVE-2023-37767-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-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	190	190
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_XReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
190.                            memcpy(&sffield, &targetField,
sizeof(GF_FieldInfo));
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=249
Status	New

The dangerous function, memcpy, was found in use at line 295 in gpac@@gpac-v2.0.0-CVE-2023-37767-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-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	335	335
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecMultipleIndexReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
335.        memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=250
Status	New

The dangerous function, memcpy, was found in use at line 591 in gpac@@gpac-v2.0.0-CVE-2023-37767-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-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	630	630
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecIndexInsert(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
630.        memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=251
Status	New

The dangerous function, memcpy, was found in use at line 831 in gpac@@gpac-v2.0.0-CVE-2023-37767-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-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	887	887
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecIndexValueReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
887.              memcpy(&sffield, &field, sizeof(GF_FieldInfo));
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=252
Status	New

The dangerous function, memcpy, was found in use at line 444 in gpac@@gpac-v2.0.0-CVE-2023-41000-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-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	485	485
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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));
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=253
Status	New

The dangerous function, memcpy, was found in use at line 732 in gpac@@gpac-v2.0.0-CVE-2023-41000-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-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	783	783
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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));
```

Dangerous Functions\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=254
Status New

The dangerous function, memcpy, was found in use at line 360 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	363	363
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
363.        memcpy(new_sr, old_sr, sizeof(SWFShapeRec));
```

Dangerous Functions\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=255
Status New

The dangerous function, memcpy, was found in use at line 360 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	369	369
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
369.              memcpy(new_sr->grad_col, old_sr->grad_col, sizeof(u32)
* old_sr->nbGrad);
```

Dangerous Functions\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=256
Status New

The dangerous function, memcpy, was found in use at line 360 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	371	371
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static SWFShapeRec *swf_clone_shape_rec(SWFShapeRec *old_sr)

```
....
371.              memcpy(new_sr->grad_ratio, old_sr->grad_ratio,
sizeof(u8) * old_sr->nbGrad);
```

Dangerous Functions\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=257
Status New

The dangerous function, memcpy, was found in use at line 377 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	430	430
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static void swf_parse_styles(SWFReader *read, u32 revision, SWFShape *shape, u32 *bits_fill, u32 *bits_line)

```
....
430.                                        memcpy(grad_col, style->grad_col, sizeof(u32) * style->nbGrad);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 377 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	431	431
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static void swf_parse_styles(SWFReader *read, u32 revision, SWFShape *shape, u32 *bits_fill, u32 *bits_line)

```
....
431.                                        memcpy(grad_ratio, style->grad_ratio, sizeof(u8) * style->nbGrad);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=259
Status	New

The dangerous function, memcpy, was found in use at line 588 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	593	593
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static void swf_append_path(SWFPath *a, SWFPath *b)

```
....
593.        memcpy(&a->pts[a->nbPts], b->pts, sizeof(SFVec2f)*b->nbPts);
```

Dangerous Functions\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=260
Status New

The dangerous function, memcpy, was found in use at line 588 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	597	597
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static void swf_append_path(SWFPath *a, SWFPath *b)

```
....
597.        memcpy(&a->types[a->nbType], b->types, sizeof(u32)*b->nbType);
```

Dangerous Functions\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=261
Status New

The dangerous function, memcpy, was found in use at line 1247 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1364	1364
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

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

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=262
Status	New

The dangerous function, memcpy, was found in use at line 1247 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1368	1368
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static GF_Err swf_place_obj(SWFReader *read, u32 revision)

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

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20

	029&pathid=263
Status	New

The dangerous function, memcpy, was found in use at line 1247 in gpac@@gpac-v2.0.0-CVE-2023-46426-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-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

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=1020036&projectid=20029&pathid=37
Status	New

The size of the buffer used by BD_XReplace in GF_FieldInfo, at line 59 of gpac@@gpac-v2.0.0-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 59 of gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	190	190
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_XReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
190.                            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=1020036&projectid=20029&pathid=38
Status	New

The size of the buffer used by BD_DecMultipleIndexReplace in GF_FieldInfo, at line 295 of gpac@@gpac-v2.0.0-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 295 of gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	335	335
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecMultipleIndexReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
335.        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=1020036&projectid=20029&pathid=39
Status	New

The size of the buffer used by BD_DecIndexInsert in GF_FieldInfo, at line 591 of gpac@@gpac-v2.0.0-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 591 of gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	630	630
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecIndexInsert(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
630.        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=1020036&projectid=20029&pathid=40
Status	New

The size of the buffer used by BD_DecIndexValueReplace in GF_FieldInfo, at line 831 of gpac@@gpac-v2.0.0-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 831 of gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	887	887
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_DecIndexValueReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
887.            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=1020036&projectid=20029&pathid=41
Status	New

The size of the buffer used by BM_ParseIndexInsert in GF_FieldInfo, at line 444 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-41000-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	485	485

Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=42
Status New

The size of the buffer used by BM_ParseIndexValueReplace in GF_FieldInfo, at line 732 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-41000-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	783	783
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=43
Status New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=44
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1364	1364
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=45
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1368	1368
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=46
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1387	1387
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=47
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1388	1388
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=48
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=49
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1364	1364
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=50
Status New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1368	1368
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=51
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1387	1387
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=52
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1388	1388
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=53
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFShapeRec, at line 360 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	363	363
Object	SWFShapeRec	SWFShapeRec

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=54
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1364	1364
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=55
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1368	1368
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=56
Status	New

The size of the buffer used by swf_place_obj in GF_Matrix2D, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1387	1387
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=57
Status	New

The size of the buffer used by swf_place_obj in GF_ColorMatrix, at line 1247 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1388	1388
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=58
Status	New

The size of the buffer used by tfra_box_read in GF_RandomAccessEntry, at line 3236 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tfra_box_read passes to GF_RandomAccessEntry, at line 3236 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err tfra_box_read(GF_Box *s, GF_BitStream *bs)

```
....
3278.             memset(p, 0, sizeof(GF_RandomAccessEntry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=59
Status	New

The size of the buffer used by trun_box_read in GF_TrunEntry, at line 7531 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that trun_box_read passes to GF_TrunEntry, at line 7531 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err trun_box_read(GF_Box *s, GF_BitStream *bs)

```
....
7564.             memset(ptr->samples, 0, sizeof(GF_TrunEntry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=60
Status	New

The size of the buffer used by udta_on_child_box in GF_UserDataMap, at line 8060 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that udta_on_child_box passes to GF_UserDataMap, at line 8060 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c

Method	GF_Err udta_on_child_box(GF_Box *s, GF_Box *a, Bool is_rem)

```
....
8085.            memset(map, 0, sizeof(GF_UserDataMap));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=61
Status	New

The size of the buffer used by subs_box_read in GF_SubSampleInfoEntry, at line 9399 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that subs_box_read passes to GF_SubSampleInfoEntry, at line 9399 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	9413	9413
Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method	GF_Err subs_box_read(GF_Box *s, GF_BitStream *bs)

```
....
9413.            memset(pSamp, 0, sizeof(GF_SubSampleInfoEntry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=62
Status	New

The size of the buffer used by subs_box_read in GF_SubSampleEntry, at line 9399 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that subs_box_read passes to GF_SubSampleEntry, at line 9399 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	9423	9423
Object	GF_SubSampleEntry	GF_SubSampleEntry

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method	GF_Err subs_box_read(GF_Box *s, GF_BitStream *bs)

```
....
9423.                   memset(pSubSamp, 0, sizeof(GF_SubSampleEntry));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=63
Status	New

The size of the buffer used by *dvcC_box_new in GF_DOVIConfigurationBox, at line 11845 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *dvcC_box_new passes to GF_DOVIConfigurationBox, at line 11845 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	11849	11849
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method	GF_Box *dvcC_box_new()

```
....
11849.      memset(tmp, 0, sizeof(GF_DOVIConfigurationBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=64
Status	New

The size of the buffer used by *dvvC_box_new in GF_DOVIConfigurationBox, at line 11929 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *dvvC_box_new passes to GF_DOVIConfigurationBox, at line 11929 of gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	11933	11933

Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Box *dvvC_box_new()

```
....
11933.      memset(tmp, 0, sizeof(GF_DOVIConfigurationBox));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=65
Status New

The size of the buffer used by *adts_dmx_probe_data in ADTSHeader, at line 884 of gpac@@gpac-v2.0.0-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 884 of gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Line	909	909
Object	ADTSHeader	ADTSHeader

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0866-TP.c
Method static const char *adts_dmx_probe_data(const u8 *data, u32 size, GF_FilterProbeScore *score)

```
....
909.        memset(&prev_hdr, 0, sizeof(ADTSHeader));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=66
Status New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 763 of gpac@@gpac-v2.0.0-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 763 of gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-	gpac@@gpac-v2.0.0-CVE-2023-2839-

	TP.c	TP.c
Line	770	770
Object	HEVCState	HEVCState

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

```
....
770.        memset(&hevc, 0, sizeof(HEVCState));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=67
Status New

The size of the buffer used by gf_bifs_dec_proto_list in GF_FieldInfo, at line 999 of gpac@@gpac-v2.0.0-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 999 of gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	1102	1102
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method GF_Err gf_bifs_dec_proto_list(GF_BifsDecoder * codec, GF_BitStream *bs, GF_List *proto_list)

```
....
1102.                    memset(&field, 0, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=68
Status New

The size of the buffer used by swf_get_matrix in GF_Matrix2D, at line 238 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	243	243
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=69
Status New

The size of the buffer used by swf_get_colormatrix in GF_ColorMatrix, at line 290 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	294	294
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=70
Status New

The size of the buffer used by *swf_clone_shape_rec in SWFPath, at line 360 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	365	365
Object	SWFPath	SWFPath

Code Snippet
File Name gpac@@gpac-v2.0.0-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 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=71
Status New

The size of the buffer used by swf_resort_path in SWFPath, at line 608 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	737	737
Object	SWFPath	SWFPath

Code Snippet
File Name gpac@@gpac-v2.0.0-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 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=72
Status New

The size of the buffer used by swf_parse_shape_def in SWFShape, at line 878 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	890	890
Object	SWFShape	SWFShape

Code Snippet
File Name gpac@@gpac-v2.0.0-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 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=73
Status New

The size of the buffer used by *swf_get_depth_entry in GF_Matrix2D, at line 1050 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1065	1065
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-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 38:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=74
Status	New

The size of the buffer used by *swf_get_depth_entry in GF_ColorMatrix, at line 1050 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1068	1068
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-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));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=75
Status	New

The size of the buffer used by swf_actions in SWFAction, at line 1088 of gpac@@gpac-v2.0.0-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_actions passes to SWFAction, at line 1088 of gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1107	1107
Object	SWFAction	SWFAction

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static GF_Err swf_actions(SWFReader *read, u32 mask, u32 key)

```
....
1107.                   memset(&act, 0, sizeof(SWFAction));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=76
Status	New

The size of the buffer used by swf_def_button in SWF_Button, at line 1180 of gpac@@gpac-v2.0.0-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_button passes to SWF_Button, at line 1180 of gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1185	1185
Object	SWF_Button	SWF_Button

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static GF_Err swf_def_button(SWFReader *read, u32 revision)

```
....
1185.       memset(&button, 0, sizeof(SWF_Button));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=77
Status	New

The size of the buffer used by swf_def_edit_text in SWFEditText, at line 1673 of gpac@@gpac-v2.0.0-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_edit_text passes to SWFEditText, at line 1673 of gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1680	1680
Object	SWFEditText	SWFEditText

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static GF_Err swf_def_edit_text(SWFReader *read)

```
....
1680.       memset(&txt, 0, sizeof(SWFEditText));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=78
Status	New

The size of the buffer used by swf_skip_soundinfo in SoundInfo, at line 1864 of gpac@@gpac-v2.0.0-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_skip_soundinfo passes to SoundInfo, at line 1864 of gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1873	1873
Object	SoundInfo	SoundInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Method static SoundInfo swf_skip_soundinfo(SWFReader *read)

```
....
1873.       memset(&si, 0, sizeof(SoundInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=79
Status	New

The size of the buffer used by avidmx_setup in GF_M4ADecSpecInfo, at line 71 of gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that avidmx_setup passes to GF_M4ADecSpecInfo, at line 71 of gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	318	318
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
318.                                    memset(&acfg, 0,
sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=80
Status	New

The size of the buffer used by mpeg2ps_stream_find_ac3_frame in GF_AC3Config, at line 849 of gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that mpeg2ps_stream_find_ac3_frame passes to GF_AC3Config, at line 849 of gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c
Line	854	854
Object	GF_AC3Config	GF_AC3Config

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c
Method static Bool mpeg2ps_stream_find_ac3_frame (mpeg2ps_stream_t *sptr)

```
....
854.        memset(&hdr, 0, sizeof(GF_AC3Config));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=81
Status	New

The size of the buffer used by get_info_from_frame in GF_AC3Config, at line 985 of gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that get_info_from_frame passes to GF_AC3Config, at line 985 of gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c
Line	1019	1019
Object	GF_AC3Config	GF_AC3Config

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c
Method static void get_info_from_frame (mpeg2ps_stream_t *sptr,

```
....
1019.                    memset(&hdr, 0, sizeof(GF_AC3Config));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=82
Status	New

The size of the buffer used by swf_get_matrix in GF_Matrix2D, at line 238 of gpac@@gpac-v2.0.0-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_get_matrix passes to GF_Matrix2D, at line 238 of gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	243	243
Object	GF_Matrix2D	GF_Matrix2D

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4720-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 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=83
Status	New

The size of the buffer used by swf_get_colormatrix in GF_ColorMatrix, at line 290 of gpac@@gpac-v2.0.0-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_get_colormatrix passes to GF_ColorMatrix, at line 290 of gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	294	294
Object	GF_ColorMatrix	GF_ColorMatrix

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4720-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 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=84
Status	New

The size of the buffer used by *swf_clone_shape_rec in SWFPath, at line 360 of gpac@@gpac-v2.0.0-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 SWFPath, at line 360 of gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	365	365
Object	SWFPath	SWFPath

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-4720-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 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=85
Status	New

The size of the buffer used by swf_resort_path in SWFPath, at line 608 of gpac@@gpac-v2.0.0-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_resort_path passes to SWFPath, at line 608 of gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	737	737
Object	SWFPath	SWFPath

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Method	static void swf_resort_path(SWFPath *a, SWFReader *read)

```
....
737.        memset(a, 0, sizeof(SWFPath));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=86
Status	New

The size of the buffer used by swf_parse_shape_def in SWFShape, at line 878 of gpac@@gpac-v2.0.0-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_parse_shape_def passes to SWFShape, at line 878 of gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	890	890
Object	SWFShape	SWFShape

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Method	static GF_Err swf_parse_shape_def(SWFReader *read, SWFFont *font, u32 revision)

```
....
890.        memset(&shape, 0, sizeof(SWFShape));
```

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=1020036&projectid=20029&pathid=31
Status	New

The application performs an illegal operation in mp3_dmx_check_dur, in gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c. In line 116, 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-v2.0.0-CVE-2023-3291-TP.c, at line 116.

	Source	Destination

File	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	157	157
Object	prev_sr	prev_sr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Method static void mp3_dmx_check_dur(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
157.                    duration /= prev_sr;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=32
Status	New

The application performs an illegal operation in mp3_dmx_check_dur, in gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c. In line 116, 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-v2.0.0-CVE-2023-3291-TP.c, at line 116.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	160	160
Object	prev_sr	prev_sr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Method static void mp3_dmx_check_dur(GF_Filter *filter, GF_MP3DmxCtx *ctx)

```
....
160.                    cur_dur /= prev_sr;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=33
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2023-0760-TP.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-2023-0760-TP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.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=1020036&projectid=20029&pathid=34
Status New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2023-0760-TP.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-2023-0760-TP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.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=1020036&projectid=20

	029&pathid=35
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2023-47465-TP.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-2023-47465-TP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-47465-TP.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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=36
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2023-47465-TP.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-2023-47465-TP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-47465-TP.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);
```

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=1020036&projectid=20029&pathid=211
Status	New

The buffer allocated by c in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-3523-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3523-TP.c
Line	313	330
Object	16	c

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=212
Status	New

The buffer allocated by c in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-3523-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3523-TP.c
Line	313	329

Object	16	c

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=213
Status	New

The buffer allocated by c in gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-3523-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3523-TP.c
Line	313	331
Object	16	c

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=820

Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	556	576
Object	continuous	continuous

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method GF_Err avidmx_process(GF_Filter *filter)

```
....
556.                    int continuous;
....
576.                    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=1020036&projectid=20029&pathid=727
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 59 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c in line 59.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	221	221
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method static GF_Err BD_XReplace(GF_BifsDecoder * codec, GF_BitStream *bs)

```
....
221.                * ((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=1020036&projectid=20029&pathid=728
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c in line 848 is not initialized when it is used by def_name at gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c in line 848.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	877	877
Object	null	def_name

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=729
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	287
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
287.                    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=1020036&projectid=20029&pathid=730
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	287
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                        st = NULL;
....
287.                    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=1020036&projectid=20029&pathid=731
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	288
Object	null	opid

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
288.                    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=1020036&projectid=20029&pathid=732
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	288
Object	null	opid

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                        st = NULL;
....
288.                    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=1020036&projectid=20029&pathid=733
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-	gpac@@gpac-v2.0.0-CVE-2023-4678-

	TP.c	TP.c
Line	258	290
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
290.                    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=1020036&projectid=20029&pathid=734
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	290
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                        st = NULL;
....
290.                    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=1020036&projectid=20029&pathid=735
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	292
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
292.                    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=1020036&projectid=20029&pathid=736
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	292
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                        st = NULL;
....
292.                    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=1020036&projectid=20029&pathid=737
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	297
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
297.                    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=1020036&projectid=20029&pathid=738
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	297
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                        st = NULL;
....
297.                    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=1020036&projectid=20029&pathid=739
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	298
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
298.                    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=1020036&projectid=20029&pathid=740
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	298
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                        st = NULL;
....
298.                    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=1020036&projectid=20029&pathid=741
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	299
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
299.                    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=1020036&projectid=20029&pathid=742
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	299
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
299.                      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=1020036&projectid=20029&pathid=743
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	301
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                      AVIAstream *st = NULL;
....
301.                      gf_filter_pid_set_property(st->opid,
GF_PROP_PID_PLAYBACK_MODE, &PROP_UINT(GF_PLAYBACK_MODE_FASTFORWARD ) );
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=744
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-	gpac@@gpac-v2.0.0-CVE-2023-4678-

	TP.c	TP.c
Line	263	301
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
301.                      gf_filter_pid_set_property(st->opid,
GF_PROP_PID_PLAYBACK_MODE, &PROP_UINT(GF_PLAYBACK_MODE_FASTFORWARD ) );
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=745
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	304
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
304.                            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=1020036&projectid=20029&pathid=746
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	304
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
304.                            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=1020036&projectid=20029&pathid=747
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	305
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
305.                            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=1020036&projectid=20029&pathid=748
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	305
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
305.                          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=1020036&projectid=20029&pathid=749
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	311
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
311.                          gf_filter_pid_set_property(st->opid,
GF_PROP_PID_TIMESCALE, &PROP_UINT(st->freq) );
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=750
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	311
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
311.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_TIMESCALE, &PROP_UINT(st->freq) );
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=751
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	325
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
325.                                  gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DECODER_CONFIG, &PROP_DATA_NO_COPY(dsi, dsi_len) );
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=752
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	325
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
325.                                  gf_filter_pid_set_property(st->opid,
GF_PROP_PID_DECODER_CONFIG, &PROP_DATA_NO_COPY(dsi, dsi_len) );
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=753
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	263	308
Object	null	opid

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
308.                                  gf_filter_pid_set_property(st->opid,
GF_PROP_PID_AUDIO_FORMAT, &PROP_UINT(afmt) );
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=754
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	308
Object	null	opid

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method	static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
308.                                  gf_filter_pid_set_property(st->opid,
GF_PROP_PID_AUDIO_FORMAT, &PROP_UINT(afmt) );
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=755
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-	gpac@@gpac-v2.0.0-CVE-2023-4678-

	TP.c	TP.c
Line	263	296
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
263.                            st = NULL;
....
296.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_BITRATE, &PROP_UINT( brate ) );
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=756
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71 is not initialized when it is used by opid at gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c in line 71.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Line	258	296
Object	null	opid

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4678-TP.c
Method static void avidmx_setup(GF_Filter *filter, GF_AVIDmxCtx *ctx)

```
....
258.                    AVIAstream *st = NULL;
....
296.                            gf_filter_pid_set_property(st->opid,
GF_PROP_PID_BITRATE, &PROP_UINT( brate ) );
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=757
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c in line 1243 is not initialized when it is used by have_dts at gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c
Line	1353	1119
Object	null	have_dts

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4681-TP.c
Method static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=758
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c in line 1243 is not initialized when it is used by have_pts at gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4681-TP.c
Line	1353	1119
Object	null	have_pts

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4681-TP.c
Method static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.               (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=759
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1271.       undef_node = NULL;
....
1327.       if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=760
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	1288	1327

Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1288.                           undef_node = NULL;
....
1327.       if (undef_node && (undef_node->sgprivate->tag == tag)) {
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=761
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1512.                                *(GF_ChildNodeItem **)info.far_ptr =
NULL;
```

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=762
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c in line 1243 is not initialized when it is used by have_dts at gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c in line 1103.

	Source	Destination

File	gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c
Line	1353	1119
Object	null	have_dts

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4721-TP.c
Method static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=763
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c in line 1243 is not initialized when it is used by have_pts at gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c in line 1103.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4721-TP.c
Line	1353	1119
Object	null	have_pts

Code Snippet
File Name gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4721-TP.c
Method static Bool add_stream (mpeg2ps_t *ps,

```
....
1119.                (ts->have_dts == 0 && ts->have_pts == 0)) {
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=764
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	1288	1327
Object	null	sgprivate

Code Snippet

File Name gpac@@gpac-v2.0.0-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 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=765
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet

File Name	gpac@@gpac-v2.0.0-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 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=766
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Method	GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1512.                                   *(GF_ChildNodeItem **)info.far_ptr =
NULL;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=767
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	1288	1327

Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v2.0.0-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 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=768
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by sgprivate at gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c in line 1247.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	1271	1327
Object	null	sgprivate

Code Snippet
File Name gpac@@gpac-v2.0.0-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 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=769
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c in line 1247 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c in line 1247.

	Source	Destination

File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	1512	1512
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Method GF_Node *gf_bt_sf_node(GF_BTParser *parser, char *node_name, GF_Node *parent, char *szDEFName)

```
....
1512.                                   *(GF_ChildNodeItem **)info.far_ptr =
NULL;
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=770
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=771
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=772
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=773
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=774
Status New

The variable declared in pa at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 739 is not initialized when it is used by type at gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c in line 739.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	741	746
Object	pa	type

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method static void naludmx_add_param_nalu(GF_List *param_list, GF_NALUFFParam *sl, u8 nal_type)

```
....
741.        GF_NALUFFParamArray *pa = NULL;
....
746.              if (pa->type == nal_type) break;
```

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=1020036&projectid=20029&pathid=686
Status	New

The naludmx_process method calls the sprintf function, at line 2769 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3559	3559
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3559.              sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->log_name, 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=1020036&projectid=20029&pathid=687
Status	New

The id3dmx_flush method calls the sprintf function, at line 223 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	324	324
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
324.                    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=1020036&projectid=20029&pathid=688
Status	New

The gf_bifs_dec_proto_list method calls the sprintf function, at line 999 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	1033	1033
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method GF_Err gf_bifs_dec_proto_list(GF_BifsDecoder * codec, GF_BitStream *bs, GF_List *proto_list)

```
....
1033.                   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=1020036&projectid=20029&pathid=689
Status	New

The gf_bifs_dec_proto_list method calls the sprintf function, at line 999 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-37767-TP.c	gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Line	1057	1057
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-37767-TP.c
Method GF_Err gf_bifs_dec_proto_list(GF_BifsDecoder * codec, GF_BitStream *bs, GF_List *proto_list)

```
....
1057.                           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=1020036&projectid=20029&pathid=690
Status New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2667	2667
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=691
Status New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2669	2669

Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=692
Status	New

The swf_def_sound method calls the sprintf function, at line 1790 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1820	1820
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=693
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c

Line	1962	1962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=694
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	1964	1964
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=695
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2079	2079
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=696
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2081	2081
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=697
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2155	2155
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=698
Status New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2157	2157
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=699
Status New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=700
Status New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=701

Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2667	2667
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=702
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2669	2669
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=703
Status	New

The swf_def_sound method calls the sprintf function, at line 1790 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1820	1820
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=704
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1962	1962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=705
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	1964	1964
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=706
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2079	2079
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=707
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2081	2081
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=708
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2155	2155
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=709
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2157	2157
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=710
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2667	2667
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=711
Status	New

The gf_sm_load_init_swf method calls the sprintf function, at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2669	2669
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=712
Status	New

The swf_def_sound method calls the sprintf function, at line 1790 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c

Line	1820	1820
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=713
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1962	1962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=714
Status	New

The swf_soundstream_hdr method calls the sprintf function, at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	1964	1964
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=715
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2079	2079
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=716
Status	New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2081	2081
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=717
Status New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2155	2155
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=718
Status New

The swf_def_bits_jpeg method calls the sprintf function, at line 2054 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2157	2157
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=719
Status New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=720
Status New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=721
Status New

The gf_bt_sffield method calls the sprintf function, at line 809 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	951	951
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20

	029&pathid=722
Status	New

The gf_bt_parse_proto method calls the sprintf function, at line 1712 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	1858	1858
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=723
Status	New

The isor_set_sample_groups_and_aux_data method calls the sprintf function, at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-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-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	946	946
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
946.                 if (grp_parameter) sprintf(szPName, "grp_%s_%d",
gf_4cc_to_str(grp_type), grp_parameter);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=724
Status	New

The isor_set_sample_groups_and_aux_data method calls the sprintf function, at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-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-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	947	947
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
947.                else sprintf(szPName, "grp_%s",
gf_4cc_to_str(grp_type));
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=725
Status	New

The isor_set_sample_groups_and_aux_data method calls the sprintf function, at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-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-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	962	962
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
962.              if (sai_parameter) sprintf(szPName, "sai_%s_%d",
gf_4cc_to_str(sai_type), sai_parameter);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=726
Status	New

The isor_set_sample_groups_and_aux_data method calls the sprintf function, at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-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-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	963	963
Object	sprintf	sprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c

Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
963.              else sprintf(szPName, "sai_%s",
gf_4cc_to_str(sai_type));
```

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=1020036&projectid=20029&pathid=796
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c

Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err cprt_box_read(GF_Box *s,GF_BitStream *bs)

```
....
248.              ptr->notice[bytesToRead] = 0;
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=797
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c	gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Line	2603	2603
Object	length	length

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-0760-TP.c
Method GF_Err payt_box_read(GF_Box *s, GF_BitStream *bs)

```
....
2603.       ptr->payloadString[length] = 0;
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=798
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	912	912
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c

Method	GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
912.                            dep->dependent_on_layerID[dep-
>num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=799
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c	gpac@@gpac-v2.0.0-CVE-2023-41000-TP.c
Line	212	212
Object	count	count

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=800
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=801
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=802
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=803
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=804
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	536	536
Object	j	j

Code Snippet
File Name gpac@@gpac-v2.0.0-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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=805

Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4683-TP.c
Line	3210	3210
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v2.0.0-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 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=806
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet
File Name gpac@@gpac-v2.0.0-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 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=807
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c

Line	502	502
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=808
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=809
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=810
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	536	536
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v2.0.0-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 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=811
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Method	GF_Err cprt_box_read(GF_Box *s,GF_BitStream *bs)

```
....
248.              ptr->notice[bytesToRead] = 0;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=812
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c	gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Line	2603	2603
Object	length	length

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-47465-TP.c
Method GF_Err payt_box_read(GF_Box *s, GF_BitStream *bs)

```
....
2603.       ptr->payloadString[length] = 0;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=813
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	498	498
Object	nbType	nbType

Code Snippet
File Name gpac@@gpac-v2.0.0-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=814
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	502	502
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=815
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=816

Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	509	509
Object	nbPts	nbPts

Code Snippet
File Name gpac@@gpac-v2.0.0-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 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=817
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	536	536
Object	j	j

Code Snippet
File Name gpac@@gpac-v2.0.0-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 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=818
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4756-TP.c

Line	3210	3210
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v2.0.0-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 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=819
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Line	3210	3210
Object	NbODs	NbODs

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-4778-TP.c
Method void gf_bt_parse_od_command(GF_BTParser *parser, char *name)

```
....
3210.                           odR->OD_ID[odR->NbODs] = id;
```

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=1020036&projectid=20029&pathid=775
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 2769 of gpac@@gpac-v2.0.0-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 2769 of gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c	gpac@@gpac-v2.0.0-CVE-2023-2839-TP.c
Line	3559	3559
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-v2.0.0-CVE-2023-2839-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
3559.              sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->log_name, 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=1020036&projectid=20029&pathid=776
Status	New

The size of the buffer used by id3dmx_flush in "tag_%s", at line 223 of gpac@@gpac-v2.0.0-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 223 of gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c	gpac@@gpac-v2.0.0-CVE-2023-3291-TP.c
Line	324	324
Object	"tag_%s"	"tag_%s"

Code Snippet
File Name gpac@@gpac-v2.0.0-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)

```
....
324.                   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=1020036&projectid=20029&pathid=777
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-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2667	2667
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=778
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c
Line	2669	2669
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=779
Status	New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=780
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-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=781
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-v2.0.0-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-v2.0.0-CVE-2023-46426-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-46426-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=782
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-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2667	2667
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=783
Status New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c
Line	2669	2669
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=784
Status New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=785
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-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=786
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-v2.0.0-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-v2.0.0-CVE-2023-4720-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4720-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=787
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-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2667	2667
Object	"%s%c%s.svg"	"%s%c%s.svg"

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=788
Status	New

The size of the buffer used by gf_sm_load_init_swf in "%s.svg", at line 2622 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c
Line	2669	2669
Object	"%s.svg"	"%s.svg"

Code Snippet
File Name gpac@@gpac-v2.0.0-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=1020036&projectid=20029&pathid=789
Status New

The size of the buffer used by swf_soundstream_hdr in "%s/swf_soundstream_%d.mp3", at line 1922 of gpac@@gpac-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=790
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-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=791
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-v2.0.0-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-v2.0.0-CVE-2023-4754-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-4754-TP.c	gpac@@gpac-v2.0.0-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-v2.0.0-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=1020036&projectid=20029&pathid=792
Status	New

The size of the buffer used by isor_set_sample_groups_and_aux_data in "grp_%s_%d", at line 928 of gpac@@gpac-v2.0.0-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_set_sample_groups_and_aux_data passes to "grp_%s_%d", at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	946	946
Object	"grp_%s_%d"	"grp_%s_%d"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
946.              if (grp_parameter) sprintf(szPName, "grp_%s_%d",
gf_4cc_to_str(grp_type), grp_parameter);
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=793
Status	New

The size of the buffer used by isor_set_sample_groups_and_aux_data in "grp_%s", at line 928 of gpac@@gpac-v2.0.0-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_set_sample_groups_and_aux_data passes to "grp_%s", at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	947	947
Object	"grp_%s"	"grp_%s"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
947.              else sprintf(szPName, "grp_%s",
gf_4cc_to_str(grp_type));
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=794
Status	New

The size of the buffer used by isor_set_sample_groups_and_aux_data in "sai_%s_%d", at line 928 of gpac@@gpac-v2.0.0-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_set_sample_groups_and_aux_data passes to "sai_%s_%d", at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	962	962
Object	"sai_%s_%d"	"sai_%s_%d"

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c

Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
962.              if (sai_parameter) sprintf(szPName, "sai_%s_%d",
gf_4cc_to_str(sai_type), sai_parameter);
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020036&projectid=20029&pathid=795
Status	New

The size of the buffer used by isor_set_sample_groups_and_aux_data in "sai_%s", at line 928 of gpac@@gpac-v2.0.0-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_set_sample_groups_and_aux_data passes to "sai_%s", at line 928 of gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c	gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Line	963	963
Object	"sai_%s"	"sai_%s"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2023-48013-TP.c
Method void isor_set_sample_groups_and_aux_data(ISOMReader *read, ISOMChannel *ch, GF_FilterPacket *pck)

```
....
963.              else sprintf(szPName, "sai_%s",
gf_4cc_to_str(sai_type));
```

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

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';
```

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

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());
```

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025