vul_files_18 Scan Report

Project Name	vul_files_18
Scan Start	Tuesday, January 7, 2025 2:37:29 PM
Preset	Checkmarx Default
Scan Time	01h:52m:22s
Lines Of Code Scanned	294321
Files Scanned	53
Report Creation Time	Tuesday, January 7, 2025 3:36:05 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	4/1000 (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

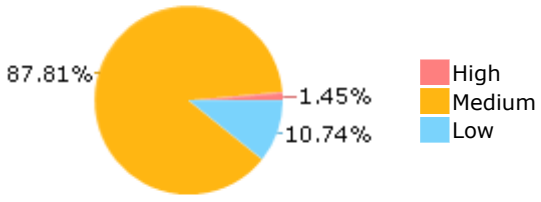
Results Limit

Results limit per query was set to 50

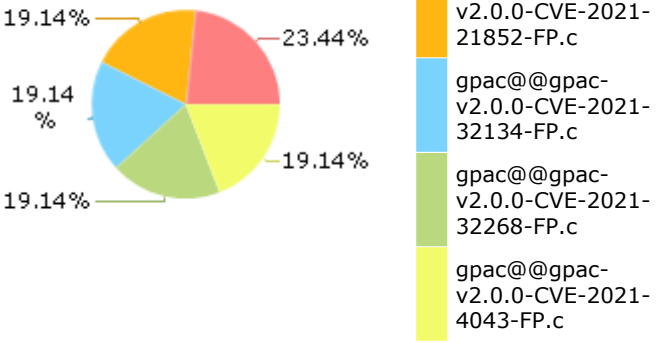
Selected Queries

Selected queries are listed in Result Summary

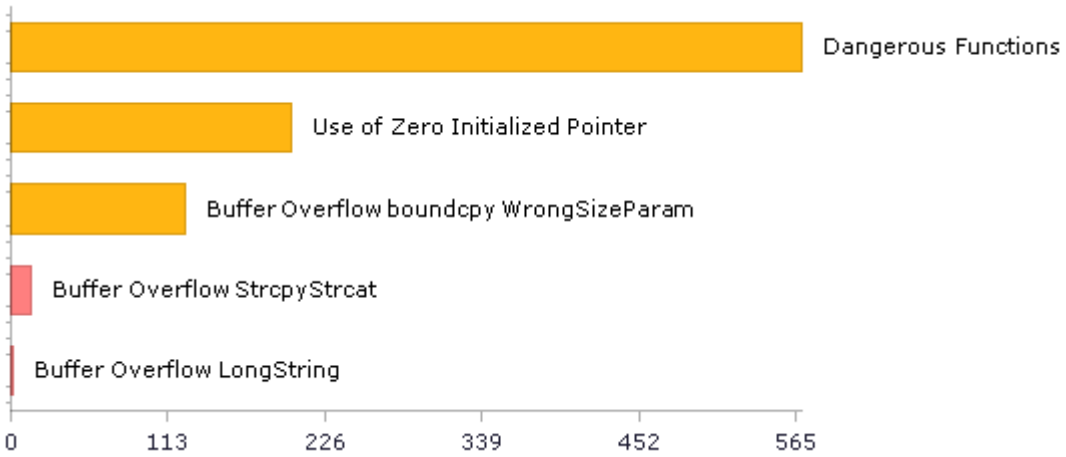
Result Summary



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	181	160
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	26	26
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	569	569
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	569	569
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

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

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	2	2
PCI DSS (3.2) - 6.5.2 - Buffer overflows	140	130
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	0	0
PCI DSS (3.2) - 6.5.4 - Insecure communications	0	0
PCI DSS (3.2) - 6.5.5 - Improper error handling*	0	0
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	0	0
PCI DSS (3.2) - 6.5.8 - Improper access control	0	0
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	0	0

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

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	0	0
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication*	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	26	26
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	0	0

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	26	26
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	237	45
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	42	32
SI-11 Error Handling (P2)*	21	21
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	2	2

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

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasnt done correctly.	0	0
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

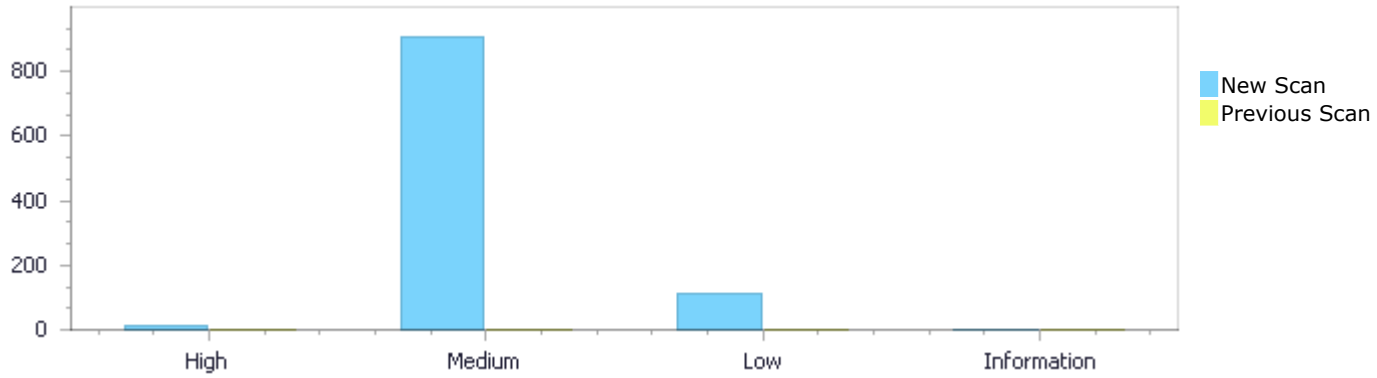
Scan Summary - Custom

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

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	15	908	111	0	1,034
Recurrent Issues	0	0	0	0	0
Total	15	908	111	0	1,034
Fixed Issues	0	0	0	0	0



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	0	0	0	0	0
To Verify	15	908	111	0	1,034
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	15	908	111	0	1,034

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	14	High
Buffer Overflow LongString	1	High
Dangerous Functions	569	Medium
Use of Zero Initialized Pointer	202	Medium
Buffer Overflow boundcpy WrongSizeParam	125	Medium

Divide By Zero	12	Medium
NULL Pointer Dereference	35	Low
Improper Resource Access Authorization	26	Low
Unchecked Array Index	23	Low
Unchecked Return Value	21	Low
Potential Precision Problem	4	Low
Potential Off by One Error in Loops	2	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	84
gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	76
gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	76
gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	76
gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	76
gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	76
gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	76
gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c	55
gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	52
gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c	36

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=1020035&projectid=20028&pathid=2
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4269
Object	mpd_src	item_path

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

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

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=3
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4269
Object	output_dir	item_path

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

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

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=4
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that revert_cache_file passes to item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4256	4269
Object	item_path	item_path

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

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

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=5
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4270
Object	mpd_src	szPATH

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

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

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

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

Method static void revert_cache_file(char *item_path)

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

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=6
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4270
Object	output_dir	szPATH

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

Method static void revert_cache_file(char *item_path)

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

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=7
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that revert_cache_file passes to item_path, at line 4256 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4256	4270
Object	item_path	szPATH

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

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

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=8
Status	New

The size of the buffer used by rip_mpd in sess, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4353
Object	mpd_src	sess

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=9
Status	New

The size of the buffer used by rip_mpd in gf_dm_sess_get_cache_name, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to mpd_src, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4353
Object	mpd_src	gf_dm_sess_get_cache_name

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=10
Status	New

The size of the buffer used by rip_mpd in output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4328
Object	output_dir	output_dir

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=11
Status	New

The size of the buffer used by rip_mpd in szName, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that rip_mpd passes to output_dir, at line 4313 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4313	4353
Object	output_dir	szName

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method	GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

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

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=12
Status	New

The size of the buffer used by xmt_parse_url in vals, at line 824 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmt_parse_string passes to name, at line 757 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	757	844
Object	name	vals

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method	static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
757.  static u32 xmt_parse_string(GF_XMTParser *parser, const char
*name, SFString *val, Bool is_mf, char *a_value)
```

File Name	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method	static u32 xmt_parse_url(GF_XMTParser *parser, const char *name, MFURL *val, GF_Node *owner, Bool is_mf, char *a_value)

```
....
844.        strcpy(value, val->vals[idx].url);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=13
Status	New

The size of the buffer used by xmt_parse_url in vals, at line 824 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmt_parse_url passes to name, at line 824 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	824	844
Object	name	vals

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static u32 xmt_parse_url(GF_XMTParser *parser, const char *name, MFURL *val, GF_Node *owner, Bool is_mf, char *a_value)

```
....
824.  static u32 xmt_parse_url(GF_XMTParser *parser, const char *name,
MFURL *val, GF_Node *owner, Bool is_mf, char *a_value)
....
844.        strcpy(value, val->vals[idx].url);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=14
Status	New

The size of the buffer used by xmt_strip_name in in, at line 1256 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmt_strip_name passes to in, at line 1256 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	1256	1259
Object	in	in

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_strip_name(const char *in, char *out)

```
....
1256.  static void xmt_strip_name(const char *in, char *out)
....
1259.       strcpy(out, in);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=15
Status	New

The size of the buffer used by xmt_strip_name in out, at line 1256 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmt_strip_name passes to out, at line 1256 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	1256	1259
Object	out	out

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_strip_name(const char *in, char *out)

```
....
1256.  static void xmt_strip_name(const char *in, char *out)
....
1259.       strcpy(out, in);
```

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=1
Status	New

The size of the buffer used by SFS_AddChar in msg, at line 90 of gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SFS_AddChar passes to "%c", at line 90 of gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	93	94
Object	"%c"	msg

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Method static void SFS_AddChar(ScriptParser *parser, char c)

```
....
93.    sprintf(msg, "%c", c);
94.    SFS_AddString(parser, msg);
```

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=1020035&projectid=20028&pathid=159
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=160
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=161
Status	New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=162
Status	New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	8089	8089
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=163
Status	New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=164
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method	GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

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

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=165
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=166
Status	New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=167
Status	New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	8089	8089

Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=168
Status	New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=169
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c

Line	681	681
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

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

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=170
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=171
Status	New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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-2021-32268-	gpac@@gpac-v2.0.0-CVE-2021-32268-

	FP.c	FP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=172
Status	New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	8089	8089
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=173
Status	New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=174
Status New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

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

Dangerous Functions\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=175
Status New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=176
Status New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=177
Status New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	8089	8089
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=178
Status New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=179
Status New

The dangerous function, memcpy, was found in use at line 444 in gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	485	485
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=180
Status	New

The dangerous function, memcpy, was found in use at line 732 in gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	783	783
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=181
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

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

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=182
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=183
Status	New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=184
Status New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	8089	8089
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=185
Status New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=186
Status New

The dangerous function, memcpy, was found in use at line 63 in gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	474	474
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
474.                    memcpy(tkc->keys[tkc->nb_keys].IV, tkc->keys[0].IV, 16);
```

Dangerous Functions\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=187
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	681	681
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Method GF_Err urn_box_read(GF_Box *s, GF_BitStream *bs)

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

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=188
Status	New

The dangerous function, memcpy, was found in use at line 645 in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	694	694
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=189
Status	New

The dangerous function, memcpy, was found in use at line 3416 in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	3428	3428
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=190
Status	New

The dangerous function, memcpy, was found in use at line 8060 in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	8089	8089
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=191
Status	New

The dangerous function, memcpy, was found in use at line 9636 in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	9777	9777
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=192
Status	New

The dangerous function, memcpy, was found in use at line 1139 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	1223	1223
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=193
Status	New

The dangerous function, memcpy, was found in use at line 1819 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	1917	1917
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=194
Status	New

The dangerous function, memcpy, was found in use at line 1819 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	1932	1932
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=195
Status	New

The dangerous function, memcpy, was found in use at line 2128 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	2138	2138
Object	memcpy	memcpy

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=196
Status	New

The dangerous function, memcpy, was found in use at line 2330 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	2476	2476
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-36186-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 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=197
Status	New

The dangerous function, memcpy, was found in use at line 2510 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	2581	2581
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-36186-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 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=198
Status	New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	2843	2843

Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=199
Status	New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	3279	3279
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=200
Status	New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-	gpac@@gpac-v2.0.0-CVE-2022-36186-

	TP.c	TP.c
Line	3484	3484
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=201
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	3493	3493
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=202
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	3502	3502
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=203
Status New

The dangerous function, memcpy, was found in use at line 2769 in gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	3520	3520
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=204
Status New

The dangerous function, memcpy, was found in use at line 454 in gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Line	502	502
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=205
Status	New

The dangerous function, memcpy, was found in use at line 454 in gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Line	547	547
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=206
Status	New

The dangerous function, memcpy, was found in use at line 384 in gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c
Line	464	464
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=207
Status	New

The dangerous function, memcpy, was found in use at line 384 in gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c
Line	474	474
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=208
Status	New

The dangerous function, memcpy, was found in use at line 384 in gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c
Line	484	484
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-47663-TP.c
Method GF_Err h263dmx_process(GF_Filter *filter)

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

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=1020035&projectid=20028&pathid=833
Status	New

The variable declared in key_info at gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c in line 1284 is not initialized when it is used by civ at gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c in line 1245.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c	gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c
Line	1347	1264
Object	key_info	civ

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c
Method GF_Err senc_Parse(GF_BitStream *bs, GF_TrackBox *trak, GF_TrackFragmentBox *traf, GF_SampleEncryptionBox *senc)

```
....
1347.             const u8 *key_info=NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c

Method	u8 key_info_get_iv_size(const u8 *key_info, u32 key_info_size, u32 idx, u8 *const_iv_size, const u8 **const_iv)

```
....
1264.                    civ = key_info + kpos + 1;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=834
Status	New

The variable declared in sub_samples at gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c in line 1516 is not initialized when it is used by sub_samples at gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c in line 1516.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Line	1528	1533
Object	sub_samples	sub_samples

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Method	u32 gf_isom_sample_get_subsample_entry(GF_ISOFile *movie, u32 track, u32 sampleNumber, u32 flags, GF_SubSampleInfoEntry **sub_sample)

```
....
1528.              sub_samples = NULL;
....
1533.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=835
Status	New

The variable declared in sub_samples at gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c in line 1516 is not initialized when it is used by sub_samples at gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c in line 1516.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Line	1519	1533
Object	sub_samples	sub_samples

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Method	u32 gf_isom_sample_get_subsample_entry(GF_ISOFile *movie, u32 track, u32 sampleNumber, u32 flags, GF_SubSampleInfoEntry **sub_sample)

```
....
1519.       GF_SubSampleInformationBox *sub_samples=NULL;
....
1533.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=836
Status	New

The variable declared in avc_state at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 412 is not initialized when it is used by avc_state at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 412.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	417	540
Object	avc_state	avc_state

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-36186-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=1020035&projectid=20028&pathid=837
Status	New

The variable declared in pa at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 739 is not initialized when it is used by pa at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 739.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c

Line	747	758
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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=1020035&projectid=20028&pathid=838
Status New

The variable declared in pa at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 739 is not initialized when it is used by pa at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 739.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	741	758
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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=1020035&projectid=20028&pathid=839
Status New

The variable declared in sub_samples at gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c in line 1516 is not initialized when it is used by sub_samples at gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c in line 1516.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c
Line	1528	1533
Object	sub_samples	sub_samples

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c
Method u32 gf_isom_sample_get_subsample_entry(GF_ISOFile *movie, u32 track, u32 sampleNumber, u32 flags, GF_SubSampleInfoEntry **sub_sample)

```
....
1528.              sub_samples = NULL;
....
1533.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=840
Status New

The variable declared in sub_samples at gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c in line 1516 is not initialized when it is used by sub_samples at gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c in line 1516.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c
Line	1519	1533
Object	sub_samples	sub_samples

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c
Method u32 gf_isom_sample_get_subsample_entry(GF_ISOFile *movie, u32 track, u32 sampleNumber, u32 flags, GF_SubSampleInfoEntry **sub_sample)

```
....
1519.       GF_SubSampleInformationBox *sub_samples=NULL;
....
1533.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=841
Status New

The variable declared in fieldValue at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 2024 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2073	772
Object	fieldValue	buffer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2073.             char *fieldValue = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
772.              if (len) val->buffer = gf_strdup(str);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=842
Status	New

The variable declared in fieldValue at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 2024 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2154	772
Object	fieldValue	buffer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2154.              char *fieldValue = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
772.               if (len) val->buffer = gf_strdup(str);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=843
Status	New

The variable declared in fieldValue at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 2024 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2154	793
Object	fieldValue	buffer

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2154.              char *fieldValue = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
793.               if (len) val->buffer = gf_strdup(str);
```

Use of Zero Initialized Pointer\Path 12:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=844
Status	New

The variable declared in fieldValue at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 2024 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2073	793
Object	fieldValue	buffer

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2073.             char *fieldValue = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
793.              if (len) val->buffer = gf_strdup(str);
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=845
Status	New

The variable declared in buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 859 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	865	870
Object	buffer	buffer

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method	static u32 xmt_parse_script(GF_XMTParser *parser, const char *name, SFScript *val, Bool is_mf, char *a_value)

```
....
865.        sfstr.buffer = NULL;
....
870.        val->script_text = (char*)sfstr.buffer;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=846
Status	New

The variable declared in buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	818	870
Object	buffer	buffer

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method	static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
818.        val->buffer = NULL;
```

File Name	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method	static u32 xmt_parse_script(GF_XMTParser *parser, const char *name, SFScript *val, Bool is_mf, char *a_value)

```
....
870.        val->script_text = (char*)sfstr.buffer;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=847
Status	New

The variable declared in buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	792	870
Object	buffer	buffer

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
792.              val->buffer = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_script(GF_XMTParser *parser, const char *name, SFScript *val, Bool is_mf, char *a_value)

```
....
870.        val->script_text = (char*)sfstr.buffer;
```

Use of Zero Initialized Pointer\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=848
Status New

The variable declared in buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 757 is not initialized when it is used by buffer at gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	771	870
Object	buffer	buffer

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
771.              val->buffer = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static u32 xmt_parse_script(GF_XMTParser *parser, const char *name, SFScript *val, Bool is_mf, char *a_value)

```
....
870.        val->script_text = (char*)sfstr.buffer;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=849
Status	New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=850
Status	New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=851
Status New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=852
Status New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=853
Status New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 22:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=854
Status	New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=855
Status	New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=856
Status	New

The variable declared in entries at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 5347 is not initialized when it is used by entries at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 5347.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	5361	5379
Object	entries	entries

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=857
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 55.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	59
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c

Method void BD_CheckSFTimeOffset(GF_BifsDecoder *codec, GF_Node *node, GF_FieldInfo *inf)

```
....
59.                BD_OffsetSFTime(codec,  (Double *)inf->far_ptr);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=858
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 55.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	61
Object	pixels	far_ptr

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c

Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c

Method void BD_CheckSFTimeOffset(GF_BifsDecoder *codec, GF_Node *node, GF_FieldInfo *inf)

```
....
61.         BD_OffsetSFTime(codec,  (Double *)inf->far_ptr);
```

Use of Zero Initialized Pointer\Path 27:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=859
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	142
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
142.                    memset(((SFString *)field->far_ptr)->buffer , 0,
length+1);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=860
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	140
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
140.                    if ( ((SFString *)field->far_ptr)->buffer )
gf_free( ((SFString *)field->far_ptr)->buffer);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=861
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	140
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
140.                    if ( ((SFString *)field->far_ptr)->buffer )
gf_free( ((SFString *)field->far_ptr)->buffer);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=862
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	150

Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
150.              SFURL *url = (SFURL *) field->far_ptr;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=863
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	181
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
181.                   gf_free(((SFImage *)field->far_ptr)->pixels);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=864
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination

File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	180
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
180.                if (((SFImage *)field->far_ptr)->pixels) {
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=865
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	203
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
203.                SFCommandBuffer *sfcb = (SFCommandBuffer *)field->far_ptr;
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=866
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	248
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
248.                    GF_Node *old_node = *((GF_Node **) field->far_ptr);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=867
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	276
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
276.              codec->LastError = node ? SFScript_Parse(codec, (SFScript*)field->far_ptr, bs, node) : GF_NON_COMPLIANT_BITSTREAM;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=868
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	283
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
283.              SFAttrRef *ar = (SFAttrRef *)field->far_ptr;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=869
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	272
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
....
272.              *((GF_Node **) field->far_ptr) = new_node;
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=870
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 506.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	523
Object	pixels	far_ptr

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c

Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c

Method GF_Err gf_bifs_dec_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
523.                          gf_node_unregister_children(node, *
(GF_ChildNodeItem **)field->far_ptr);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=871
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 301.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	360
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
```

File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c

Method GF_Err BD_DecMFFieldList(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
360.                                e = gf_node_list_add_child_last(
(GF_ChildNodeItem **)field->far_ptr, new_node, &last);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=872
Status	New

The variable declared in pixels at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by far_ptr at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 392.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	182	465
Object	pixels	far_ptr

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
182.                    ((SFImage *)field->far_ptr)->pixels = NULL;
```

File Name	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method	GF_Err BD_DecMFFieldVec(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
465.                                e = gf_node_list_add_child_last(
(GF_ChildNodeItem **)field->far_ptr, new_node, &last);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=873
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 399.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	178	433
Object	global_qp	new_node

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-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 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=874
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 399.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	177	433
Object	ActiveQP	new_node

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-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 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=875
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 43.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	178	77
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-TP.c

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

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

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=876
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 43.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	177	77
Object	ActiveQP	new_node

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-TP.c

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

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

Use of Zero Initialized Pointer\Path 45:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=877
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	177	195
Object	ActiveQP	new_node

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

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

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=878
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by new_node at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	178	195
Object	global_qp	new_node

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

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

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=879
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	177	188
Object	ActiveQP	global_qp

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

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

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=880
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	178	188
Object	global_qp	global_qp

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

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

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=881
Status	New

The variable declared in ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	177	186
Object	ActiveQP	ActiveQP

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

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

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=882
Status	New

The variable declared in global_qp at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165 is not initialized when it is used by ActiveQP at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 165.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c

Line	178	186
Object	global_qp	ActiveQP

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Method static GF_Err BM_ParseGlobalQuantizer(GF_BifsDecoder *codec, GF_BitStream *bs, GF_List *com_list)

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

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=1020035&projectid=20028&pathid=30
Status	New

The size of the buffer used by BM_ParseIndexInsert in GF_FieldInfo, at line 444 of gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	485	485
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=31
Status	New

The size of the buffer used by BM_ParseIndexValueReplace in GF_FieldInfo, at line 732 of gpac@@gpac-v2.0.0-CVE-2022-1795-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-2022-1795-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	783	783
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=32
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=33
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=34
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=35
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	9413	9413
Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=36
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	9423	9423
Object	GF_SubSampleEntry	GF_SubSampleEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=37
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	11849	11849
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Method GF_Box *dvcC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=38
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-2021-21852-FP.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-2021-21852-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	11933	11933
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Method GF_Box *dvvC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=39
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=40
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=41
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=42
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	9413	9413

Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=43
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	9423	9423
Object	GF_SubSampleEntry	GF_SubSampleEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.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 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=44
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-	gpac@@gpac-v2.0.0-CVE-2021-32134-

	FP.c	FP.c
Line	11849	11849
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method GF_Box *dvcC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=45
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-2021-32134-FP.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-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	11933	11933
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method GF_Box *dvvC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=46
Status	New

The size of the buffer used by dump_mpeg2_ts in GF_M2TS_Dump, at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_mpeg2_ts passes to GF_M2TS_Dump, at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4142	4142
Object	GF_M2TS_Dump	GF_M2TS_Dump

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4142.       memset(&dumper, 0, sizeof(GF_M2TS_Dump));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=47
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=48
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=49
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=50
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	9413	9413
Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=51
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	9423	9423
Object	GF_SubSampleEntry	GF_SubSampleEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.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 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=52
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	11849	11849
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method GF_Box *dvcC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=53
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-2021-32268-FP.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-2021-32268-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	11933	11933
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method GF_Box *dvvC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=54
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=55
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 27:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=56
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=57
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	9413	9413
Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 29:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=58
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	9423	9423
Object	GF_SubSampleEntry	GF_SubSampleEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.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 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=59
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	11849	11849
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method GF_Box *dvcC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=60
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-2021-4043-FP.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-2021-4043-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	11933	11933
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method GF_Box *dvvC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=61
Status	New

The size of the buffer used by BD_DecMFFieldList in GF_FieldInfo, at line 301 of gpac@@gpac-v2.0.0-CVE-2022-1172-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_DecMFFieldList passes to GF_FieldInfo, at line 301 of gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	311	311
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err BD_DecMFFieldList(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
311.        memset(&sffield, 0, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=62
Status	New

The size of the buffer used by BD_DecMFFieldVec in GF_FieldInfo, at line 392 of gpac@@gpac-v2.0.0-CVE-2022-1172-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_DecMFFieldVec passes to GF_FieldInfo, at line 392 of gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	401	401
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err BD_DecMFFieldVec(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
401.        memset(&sffield, 0, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=63
Status	New

The size of the buffer used by gppc_box_read in GF_3GPConfig, at line 48 of gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gppc_box_read passes to GF_3GPConfig, at line 48 of gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c
Line	52	52
Object	GF_3GPConfig	GF_3GPConfig

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c
Method	GF_Err gppc_box_read(GF_Box *s, GF_BitStream *bs)

```
....
52.    memset(&ptr->cfg, 0, sizeof(GF_3GPConfig));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=64
Status	New

The size of the buffer used by BD_DecMFFieldList in GF_FieldInfo, at line 301 of gpac@@gpac-v2.0.0-CVE-2022-2453-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_DecMFFieldList passes to GF_FieldInfo, at line 301 of gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c
Line	311	311
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c
Method	GF_Err BD_DecMFFieldList(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
311.        memset(&sffield, 0, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=65
Status	New

The size of the buffer used by BD_DecMFFieldVec in GF_FieldInfo, at line 392 of gpac@@gpac-v2.0.0-CVE-2022-2453-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_DecMFFieldVec passes to GF_FieldInfo, at line 392 of gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c
Line	401	401
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c
Method GF_Err BD_DecMFFieldVec(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
401.        memset(&sffield, 0, sizeof(GF_FieldInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=66
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=67
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c

Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=68
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=69
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-	gpac@@gpac-v2.0.0-CVE-2022-24577-

	FP.c	FP.c
Line	9413	9413
Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=70
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	9423	9423
Object	GF_SubSampleEntry	GF_SubSampleEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.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 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=71
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	11849	11849
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Box *dvcC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=72
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-2022-24577-FP.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-2022-24577-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	11933	11933
Object	GF_DOVIConfigurationBox	GF_DOVIConfigurationBox

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Box *dvvC_box_new()

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

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=73
Status New

The size of the buffer used by cryptinfo_node_start in GF_CryptKeyInfo, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that cryptinfo_node_start passes to GF_CryptKeyInfo, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	107	107
Object	GF_CryptKeyInfo	GF_CryptKeyInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
107.              memset(tkc->keys, 0, sizeof(GF_CryptKeyInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=74
Status New

The size of the buffer used by cryptinfo_node_start in GF_CryptKeyInfo, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that cryptinfo_node_start passes to GF_CryptKeyInfo, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	422	422
Object	GF_CryptKeyInfo	GF_CryptKeyInfo

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
422.                    memset(&tkc->keys[tkc->nb_keys], 0,
sizeof(GF_CryptKeyInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=75

Status	New

The size of the buffer used by *gf_isom_new_movie in GF_ISOFile, at line 860 of gpac@@gpac-v2.0.0-CVE-2022-29340-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_isom_new_movie passes to GF_ISOFile, at line 860 of gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Line	867	867
Object	GF_ISOFile	GF_ISOFile

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Method GF_ISOFile *gf_isom_new_movie()

```
....
867.        memset(mov, 0, sizeof(GF_ISOFile));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=76
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-2022-3178-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-2022-3178-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	3278	3278
Object	GF_RandomAccessEntry	GF_RandomAccessEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=77
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-2022-3178-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-2022-3178-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	7564	7564
Object	GF_TrunEntry	GF_TrunEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=78
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-2022-3178-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-2022-3178-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	8085	8085
Object	GF_UserDataMap	GF_UserDataMap

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 50:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=79
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-2022-3178-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-2022-3178-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	9413	9413
Object	GF_SubSampleInfoEntry	GF_SubSampleInfoEntry

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Method GF_Err subs_box_read(GF_Box *s, GF_BitStream *bs)

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

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=1020035&projectid=20028&pathid=16
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7812.             if (ctrn->ctso_multiplier) return
ctrn_s32_to_index(ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=17
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7816.       if (ctrn->ctso_multiplier) return
ctrn_u32_to_index((u32)ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=18
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	7812	7812

Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7812.             if (ctrn->ctso_multiplier) return
ctrn_s32_to_index(ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=19
Status New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7816.       if (ctrn->ctso_multiplier) return
ctrn_u32_to_index((u32)ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=20
Status New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7812.             if (ctrn->ctso_multiplier) return
ctrn_s32_to_index(ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=21
Status New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7816.       if (ctrn->ctso_multiplier) return
ctrn_u32_to_index((u32)ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=22
Status New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7812.             if (ctrn->ctso_multiplier) return
ctrn_s32_to_index(ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=23
Status New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7816.       if (ctrn->ctso_multiplier) return
ctrn_u32_to_index((u32)ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 9:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=24
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7812.             if (ctrn->ctso_multiplier) return
ctrn_s32_to_index(ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=25
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c. In line 7804, the program attempts to divide by ctso_multiplier, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ctso_multiplier in ctrn_ctts_to_index of gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	7816	7816
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method static u32 ctrn_ctts_to_index(GF_TrackFragmentRunBox *ctrn, s32 ctts)

```
....
7816.       if (ctrn->ctso_multiplier) return
ctrn_u32_to_index((u32)ctts / ctrn->ctso_multiplier);
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=26
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	7812	7812
Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=27
Status	New

The application performs an illegal operation in ctrn_ctts_to_index, in gpac@@gpac-v2.0.0-CVE-2022-3178-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-2022-3178-TP.c, at line 7804.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	7816	7816

Object	ctso_multiplier	ctso_multiplier

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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);
```

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=1020035&projectid=20028&pathid=775
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Line	262	262
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1172-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
262.                        *((GF_Node **) field->far_ptr) = NULL;
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=776
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 848 is not initialized when it is used by def_name at gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c in line 848.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	877	877
Object	null	def_name

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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=1020035&projectid=20028&pathid=777
Status New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c in line 75 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c	gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c
Line	262	262
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-2453-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
262.                          *((GF_Node **) field->far_ptr) = NULL;
```

NULL Pointer Dereference\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=778

Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	179	179
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Method GF_Err SFScript_Parse(GF_BifsDecoder *codec, SFScript *script_field, GF_BitStream *bs, GF_Node *n)

```
....
179.        parser.new_line = (char *) (codec->dec_memory_mode ? "\n" :
NULL);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=779
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	179	202
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Method GF_Err SFScript_Parse(GF_BifsDecoder *codec, SFScript *script_field, GF_BitStream *bs, GF_Node *n)

```
....
179.        parser.new_line = (char *) (codec->dec_memory_mode ? "\n" :
NULL);
....
202.        SFS_AddString(&parser, parser.new_line);
```

NULL Pointer Dereference\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=780
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by string at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 70.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	179	81
Object	null	string

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method GF_Err SFScript_Parse(GF_BifsDecoder *codec, SFScript *script_field, GF_BitStream *bs, GF_Node *n)

```
....
179.        parser.new_line = (char *) (codec->dec_memory_mode ? "\n" :
NULL);
```

File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
81.   strncat(parser->string, str, parser->length - strlen(parser-
>string) - 1);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=781
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by string at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 70.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	179	81
Object	null	string

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Method GF_Err SFScript_Parse(GF_BifsDecoder *codec, SFScript *script_field, GF_BitStream *bs, GF_Node *n)

```
....
179.        parser.new_line = (char *) (codec->dec_memory_mode ? "\n" :
NULL);
```

File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
81.   strncat(parser->string, str, parser->length - strlen(parser-
>string) - 1);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=782
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 145.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	179	146
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Method GF_Err SFScript_Parse(GF_BifsDecoder *codec, SFScript *script_field, GF_BitStream *bs, GF_Node *n)

```
....
179.        parser.new_line = (char *) (codec->dec_memory_mode ? "\n" :
NULL);
```

File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method static void SFS_Space(ScriptParser *pars) {

```
....
146.        if (pars->new_line) SFS_AddString(pars, " ");
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=783
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by length at gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c in line 70.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	179	81
Object	null	length

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method GF_Err SFScript_Parse(GF_BifsDecoder *codec, SFScript *script_field, GF_BitStream *bs, GF_Node *n)

```
....
179.        parser.new_line = (char *) (codec->dec_memory_mode ? "\n" :
NULL);
```

File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
81.   strncat(parser->string, str, parser->length - strlen(parser-
>string) - 1);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=784
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-43043-TP.c in line 75 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2022-43043-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43043-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43043-TP.c
Line	262	262

Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43043-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
262.                            *((GF_Node **) field->far_ptr) = NULL;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=785
Status	New

The variable declared in null at gpac@@gpac-v2.0.0-CVE-2022-45343-TP.c in line 75 is not initialized when it is used by Pointer at gpac@@gpac-v2.0.0-CVE-2022-45343-TP.c in line 75.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-45343-TP.c	gpac@@gpac-v2.0.0-CVE-2022-45343-TP.c
Line	262	262
Object	null	Pointer

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-45343-TP.c
Method GF_Err gf_bifs_dec_sf_field(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
262.                            *((GF_Node **) field->far_ptr) = NULL;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=786
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c

Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=787
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=788
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c

Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=789
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=790
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c

Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=791
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=792
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c

Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=793
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=794
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c

Line	3063	3063
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=795
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=796
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 402 is not initialized when it is used by Marker at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 402.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c

Line	418	418
Object	0	Marker

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_avc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
418.                builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=797
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 402 is not initialized when it is used by builder at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 402.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	418	431
Object	0	builder

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_avc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
418.                builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
....
431.                builder->OnNewPacket(builder->cbk_obj, &builder->rtp_header);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=798
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 402 is not initialized when it is used by rtp_header at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 402.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	418	431
Object	0	rtp_header

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_avc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
418.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
....
431.              builder->OnNewPacket(builder->cbk_obj, &builder-
>rtp_header);
```

NULL Pointer Dereference\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=799
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 538 is not initialized when it is used by Marker at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 538.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	551	551
Object	0	Marker

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_hevc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
551.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=800
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 538 is not initialized when it is used by rtp_header at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 538.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	551	568
Object	0	rtp_header

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_hevc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
551.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
....
568.              builder->OnNewPacket(builder->cbk_obj, &builder-
>rtp_header);
```

NULL Pointer Dereference\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=801
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 538 is not initialized when it is used by builder at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 538.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	551	568
Object	0	builder

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_hevc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
551.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
....
568.              builder->OnNewPacket(builder->cbk_obj, &builder-
>rtp_header);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=802
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 693 is not initialized when it is used by Marker at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 693.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	706	706
Object	0	Marker

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_vvc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
706.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=803
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 693 is not initialized when it is used by rtp_header at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 693.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	706	723
Object	0	rtp_header

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_vvc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
706.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
....
723.              builder->OnNewPacket(builder->cbk_obj, &builder-
>rtp_header);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=804
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 693 is not initialized when it is used by builder at gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c in line 693.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Line	706	723
Object	0	builder

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29537-TP.c
Method GF_Err gp_rtp_builder_do_vvc(GP_RTPPacketizer *builder, u8 *nalu, u32 nalu_size, u8 IsAUEnd, u32 FullAUSize)

```
....
706.              builder->rtp_header.Marker = (do_flush==1) ? 1 : 0;
....
723.              builder->OnNewPacket(builder->cbk_obj, &builder-
>rtp_header);
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=805
Status	New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c in line 3060 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c in line 3060.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	3063	3063

Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Method GF_Err mdhd_box_size(GF_Box *s)

```
....
3063.       ptr->version = (ptr->duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=806
Status New

The variable declared in 0 at gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c in line 4547 is not initialized when it is used by version at gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c in line 4547.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	4550	4550
Object	0	version

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Method GF_Err mehd_box_size(GF_Box *s)

```
....
4550.       ptr->version = (ptr->fragment_duration>0xFFFFFFFF) ? 1 : 0;
```

NULL Pointer Dereference\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=807
Status New

The variable declared in pSamp at gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c in line 1436 is not initialized when it is used by sample_delta at gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c in line 1436.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c	gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Line	1439	1448

Object	pSamp	sample_delta

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-29340-TP.c
Method GF_Err gf_isom_add_subsample_info(GF_SubSampleInformationBox *sub_samples, u32 sampleNumber, u32 subSampleSize, u8 priority, u32 reserved, Bool discardable)

```
....
1439.       GF_SubSampleInfoEntry *pSamp;
....
1448.             if (last_sample + pSamp->sample_delta > sampleNumber)
return GF_NOT_SUPPORTED;
```

NULL Pointer Dereference\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=808
Status New

The variable declared in pa at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 739 is not initialized when it is used by type at gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c in line 739.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	741	746
Object	pa	type

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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;
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=809
Status New

The variable declared in pSamp at gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c in line 1436 is not initialized when it is used by sample_delta at gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c in line 1436.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c
Line	1439	1448
Object	pSamp	sample_delta

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43254-TP.c
Method GF_Err gf_isom_add_subsample_info(GF_SubSampleInformationBox *sub_samples, u32 sampleNumber, u32 subSampleSize, u8 priority, u32 reserved, Bool discardable)

```
....
1439.       GF_SubSampleInfoEntry *pSamp;
....
1448.             if (last_sample + pSamp->sample_delta > sampleNumber)
return GF_NOT_SUPPORTED;
```

Improper Resource Access Authorization

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

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description
Improper Resource Access Authorization\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=728
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4347	4347
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4347.       fprintf(stderr, "Downloading %s\n", mpd_src);
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=729
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4440	4440
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4440.                           fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=730
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4468	4468
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
4468.                               fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20

	028&pathid=731
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3933	3933
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3933.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=732
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3938	3938
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3938.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=733
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3946	3946
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3946.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=734
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3952	3952
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3952.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=735
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-	gpac@@gpac-v2.0.0-CVE-2021-32136-

	FP.c	FP.c
Line	3957	3957
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3957.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=736
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3962	3962
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3962.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=737
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3986	3986

Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3986.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=738
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	3994	3994
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3994.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=739
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4002	4002
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4002.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=740
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4059	4059
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4059.                          fprintf(dumper->timestamps_info_file,
"%u\t%d\t", pck->stream->pes_start_packet_number, pck->stream->pid);
```

Improper Resource Access Authorization\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=741
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4060	4060
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4060.                           if (interpolated_pcr_value)
fprintf(dumper->timestamps_info_file, "%f",
interpolated_pcr_value/(300.0 * 90000));
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=742
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4061	4061
Object	fprintf	fprintf

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4061.                           fprintf(dumper->timestamps_info_file,
"\t");
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=743
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4062	4062
Object	fprintf	fprintf

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4062.                          if (pck->DTS) fprintf(dumper-
>timestamps_info_file, "%f", (pck->DTS / 90000.0));
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=744
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4063	4063
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4063.                          fprintf(dumper->timestamps_info_file,
"\t%f\t%d\t%d", pck->PTS / 90000.0, (pck->flags & GF_M2TS_PES_PCK_RAP) ?
1 : 0, (pck->flags & GF_M2TS_PES_PCK_DISCONTINUITY) ? 1 : 0);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=745
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4067	4067
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4067.                                   fprintf(dumper-
>timestamps_info_file, "\t%f\n", diff);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=746
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4072	4072
Object	fprintf	fprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4072.                                   fprintf(dumper-
>timestamps_info_file, "\t\n");
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=747
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4086	4086
Object	fprintf	fprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
4086.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\t%f\t\t\t\t%d\n", pck->stream->program-
>last_pcr_value_pck_number, pck->stream->pid, pck->PTS / (300*90000.0),
(pck->flags & GF_M2TS_PES_PCK_DISCONTINUITY) ? 1 : 0);
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=748
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4131	4131
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4131.             fprintf(stderr, "No program number nor output filename
specified. No timestamp file will be generated.");
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=749
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4181	4181
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4181.             fprintf(stderr, "No program number specified,
defaulting to first program\n");
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=750
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4185	4185
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4185.             fprintf(stderr, "No program number nor output filename
specified. No timestamp file will be generated\n");
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=751
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4195	4195
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4195.             fprintf(dumper.timestamps_info_file,
"PCK#\tPID\tPCR\tDTS\tPTS\tRAP\tDiscontinuity\tDTS-PCR Diff\n");
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=752
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4238	4238
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void get_file_callback(void *usr_cbk, GF_NETIO_Parameter *parameter)

```
....
4238.                    fprintf(stderr, "download %02d %% at %05d
kpbs\r", (u32) max, bps*8/1000);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=753
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4263	4263
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

```
....
4263.              fprintf(stderr, "%s is not a gpac cache file\n",
item_path);
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=810
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=811
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c	gpac@@gpac-v2.0.0-CVE-2021-21852-FP.c
Line	2603	2603
Object	length	length

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-21852-FP.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=1020035&projectid=20028&pathid=812
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c	gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c
Line	154	154
Object	len	len

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-31254-FP.c
Method GF_Err schm_box_read(GF_Box *s, GF_BitStream *bs)

```
....
154.                ptr->URI[len] = 0;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=813
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method GF_Err cprt_box_read(GF_Box *s,GF_BitStream *bs)

```
....
248.                ptr->notice[bytesToRead] = 0;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=814
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32134-	gpac@@gpac-v2.0.0-CVE-2021-32134-

	FP.c	FP.c
Line	2603	2603
Object	length	length

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32134-FP.c
Method GF_Err payt_box_read(GF_Box *s, GF_BitStream *bs)

```
....
2603.       ptr->payloadString[length] = 0;
```

Unchecked Array Index\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=815
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method GF_Err cprt_box_read(GF_Box *s,GF_BitStream *bs)

```
....
248.              ptr->notice[bytesToRead] = 0;
```

Unchecked Array Index\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=816
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Line	2603	2603
Object	length	length

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2021-32268-FP.c
Method	GF_Err payt_box_read(GF_Box *s, GF_BitStream *bs)

```
....
2603.       ptr->payloadString[length] = 0;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=817
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method	GF_Err cprt_box_read(GF_Box *s,GF_BitStream *bs)

```
....
248.              ptr->notice[bytesToRead] = 0;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=818
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Line	2603	2603
Object	length	length

Code Snippet

File Name	gpac@@gpac-v2.0.0-CVE-2021-4043-FP.c
Method	GF_Err payt_box_read(GF_Box *s, GF_BitStream *bs)

```
....
2603.       ptr->payloadString[length] = 0;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=819
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c
Line	396	396
Object	i	i

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c
Method GF_Err text_box_read(GF_Box *s, GF_BitStream *bs)

```
....
396.                            ptr->textName[i] = c;
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=820
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c
Line	410	410
Object	i	i

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1441-TP.c
Method GF_Err text_box_read(GF_Box *s, GF_BitStream *bs)

```
....
410.                ptr->textName[i] = '\0';                                /*Font
name*/
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=821

Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c	gpac@@gpac-v2.0.0-CVE-2022-1795-TP.c
Line	212	212
Object	count	count

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-1795-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 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=822
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c	gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Err cprt_box_read(GF_Box *s,GF_BitStream *bs)

```
....
248.             ptr->notice[bytesToRead] = 0;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=823
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-24577-	gpac@@gpac-v2.0.0-CVE-2022-24577-

	FP.c	FP.c
Line	2603	2603
Object	length	length

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-24577-FP.c
Method GF_Err payt_box_read(GF_Box *s, GF_BitStream *bs)

```
....
2603.       ptr->payloadString[length] = 0;
```

Unchecked Array Index\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=824
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	286	286
Object	l	l

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
286.                            tkc->metadata[l] = 0;
```

Unchecked Array Index\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=825
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	248	248
Object	bytesToRead	bytesToRead

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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=1020035&projectid=20028&pathid=826
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3178-TP.c
Line	2603	2603
Object	length	length

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3178-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=1020035&projectid=20028&pathid=827
Status New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	912	912
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-36186-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 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=828
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	808	808
Object	k	k

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
808.                    value[k] = str[i];
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=829
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	814	814
Object	k	k

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static u32 xmt_parse_string(GF_XMTParser *parser, const char *name, SFString *val, Bool is_mf, char *a_value)

```
....
814.        value[k] = 0;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=830
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2425	2425
Object	del_proto_list_size	del_proto_list_size

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2425.                                   parser->command-
>del_proto_list[parser->command->del_proto_list_size] = p->ID;
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=831
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2497	2497
Object	NbESDs	NbESDs

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2497.                                   esdR->ES_ID[esdR->NbESDs] = es_id;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=832
Status	New

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	2516	2516
Object	NbODs	NbODs

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2516.                                   odR->OD_ID[odR->NbODs] = od_id;
```

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=1020035&projectid=20028&pathid=754
Status	New

The dump_mpeg2_ts method calls the sprintf function, at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4152	4152
Object	sprintf	sprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c

Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4152.                    sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=755
Status	New

The dump_mpeg2_ts method calls the sprintf function, at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4189	4189
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4189.             sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=756
Status	New

The gf_crypt_file_ex method calls the sprintf function, at line 711 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	727	727
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method	static GF_Err gf_crypt_file_ex(GF_ISOFile *mp4, const char *drm_file, const char *dst_file, Double interleave_time, const char *fragment_name, u32 fs_dump_flags)

```
....
727.        sprintf(an_arg, "mp4dmx:mov=%p", mp4);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=757
Status	New

The gf_crypt_file_ex method calls the sprintf function, at line 711 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	762	762
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method	static GF_Err gf_crypt_file_ex(GF_ISOFile *mp4, const char *drm_file, const char *dst_file, Double interleave_time, const char *fragment_name, u32 fs_dump_flags)

```
....
762.                    sprintf(an_arg, ":cdur=%g", interleave_time);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=758
Status	New

The cryptinfo_node_start method calls the sprintf function, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-	gpac@@gpac-v2.0.0-CVE-2022-26967-

	TP.c	TP.c
Line	143	143
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
143.                                    sprintf(szV, "%c%c", sKey[j],
sKey[j+1]);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=759
Status New

The cryptinfo_node_start method calls the sprintf function, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	233	233
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
233.                                    sprintf(szV, "%c%c", sKey[j],
sKey[j+1]);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=760
Status New

The cryptinfo_node_start method calls the sprintf function, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	311	311
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
311.                                    sprintf(szV, "%c%c", sKey[j],
sKey[j+1]);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=761
Status New

The cryptinfo_node_start method calls the sprintf function, at line 63 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	462	462
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Method static void cryptinfo_node_start(void *sax_cbck, const char *node_name, const char *name_space, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
462.                                    sprintf(szV, "%c%c", sKey[j],
sKey[j+1]);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=762
Status	New

The gf_decrypt_file_ex method calls the sprintf function, at line 580 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	595	595
Object	sprintf	sprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c

Method static GF_Err gf_decrypt_file_ex(GF_ISOFile *mp4, const char *drm_file, const char *dst_file, Double interleave_time, const char *fragment_name, u32 fs_dump_flags)

```
....
595.        sprintf(an_arg, "mp4dmx:mov=%p", mp4);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=763
Status	New

The gf_decrypt_file_ex method calls the sprintf function, at line 580 of gpac@@gpac-v2.0.0-CVE-2022-26967-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-2022-26967-TP.c	gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c
Line	630	630
Object	sprintf	sprintf

Code Snippet

File Name gpac@@gpac-v2.0.0-CVE-2022-26967-TP.c

Method static GF_Err gf_decrypt_file_ex(GF_ISOFile *mp4, const char *drm_file, const char *dst_file, Double interleave_time, const char *fragment_name, u32 fs_dump_flags)

```
....
630.                    sprintf(an_arg, ":cdur=%g", interleave_time);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=764
Status	New

The SFS_AddInt method calls the sprintf function, at line 84 of gpac@@gpac-v2.0.0-CVE-2022-3222-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-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	87	87
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Method static void SFS_AddInt(ScriptParser *parser, s32 val)

```
....
87.    sprintf(msg, "%d", val);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=765
Status	New

The SFS_AddChar method calls the sprintf function, at line 90 of gpac@@gpac-v2.0.0-CVE-2022-3222-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-2022-3222-TP.c	gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c
Line	93	93
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-3222-TP.c

Method	static void SFS_AddChar(ScriptParser *parser, char c)

```
....
93.    sprintf(msg, "%c", c);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=766
Status	New

The naludmx_process method calls the sprintf function, at line 2769 of gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c
Line	3559	3559
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-36186-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=767
Status	New

The xmt_new_od_link method calls the sprintf function, at line 181 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	192	192
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method	static void xmt_new_od_link(GF_XMTParser *parser, GF_ObjectDescriptor *od, char *name, u32 ID)

```
....
192.                    sprintf(szURL, "%u", ID);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=768
Status	New

The xmt_new_od_link_from_node method calls the sprintf function, at line 240 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	252	252
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method	static void xmt_new_od_link_from_node(GF_XMTParser *parser, char *name, MFURL *url)

```
....
252.                sprintf(szURL, "%u", ID);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=769
Status	New

The xmt_locate_stream method calls the sprintf function, at line 381 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Line	391	391
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static u32 xmt_locate_stream(GF_XMTParser *parser, char *stream_name)

```
....
391.                    sprintf(szN, "es%d", esdl->ESID);
```

Unchecked Return Value\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=770
Status New

The xmt_locate_stream method calls the sprintf function, at line 381 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	393	393
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static u32 xmt_locate_stream(GF_XMTParser *parser, char *stream_name)

```
....
393.                    sprintf(szN, "%d", esdl->ESID);
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=771
Status New

The xmt_locate_stream method calls the sprintf function, at line 381 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-	gpac@@gpac-v2.0.0-CVE-2022-43255-

	TP.c	TP.c
Line	402	402
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static u32 xmt_locate_stream(GF_XMTParser *parser, char *stream_name)

```
....
402.                    sprintf(szN, "%d", sc->ESID);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=772
Status	New

The xmt_resolve_od_links method calls the sprintf function, at line 427 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	465	465
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_resolve_od_links(GF_XMTParser *parser)

```
....
465.              sprintf(szTest, "%d", ocr_id);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=773
Status	New

The xmt_resolve_od_links method calls the sprintf function, at line 427 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	498	498
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_resolve_od_links(GF_XMTParser *parser)

```
....
498.                sprintf(szTest, "%d", dep_id);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=774
Status	New

The xmt_resolve_od_links method calls the sprintf function, at line 427 of gpac@@gpac-v2.0.0-CVE-2022-43255-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-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	585	585
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Method static void xmt_resolve_od_links(GF_XMTParser *parser)

```
....
585.                                        sprintf(szURL, "od:%d#%s", l-
>od->objectDescriptorID, seg+1);
```

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=1020035&projectid=20028&pathid=155
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_%d.raw", at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_mpeg2_ts passes to "%s_%d.raw", at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4152	4152
Object	"%s_%d.raw"	"%s_%d.raw"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4152.                    sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=156
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_prog_%d_timestamps.txt", at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that dump_mpeg2_ts passes to "%s_prog_%d_timestamps.txt", at line 4120 of gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c	gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Line	4189	4189
Object	"%s_prog_%d_timestamps.txt"	"%s_prog_%d_timestamps.txt"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
4189.              sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=157
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-2022-36186-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-2022-36186-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-36186-TP.c	gpac@@gpac-v2.0.0-CVE-2022-36186-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-2022-36186-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 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=158
Status	New

The size of the buffer used by xmt_resolve_od_links in "od:%d#%s", at line 427 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that xmt_resolve_od_links passes to "od:%d#%s", at line 427 of gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c	gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c
Line	585	585
Object	"od:%d#%s"	"od:%d#%s"

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-43255-TP.c

Method	static void xmt_resolve_od_links(GF_XMTParser *parser)

```
....
585.                                        sprintf(szURL, "od:%d#%s", l-
>od->objectDescriptorID, seg+1);
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=28
Status	New

The buffer allocated by <= in gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c at line 81 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-2022-47659-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Line	121	121
Object	<=	<=

Code Snippet	
File Name	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Method	static Bool latm_dmx_sync_frame_bs(GF_BitStream *bs, GF_M4ADecSpecInfo *acfg, u32 *nb_bytes, u8 *buffer, u32 *nb_skipped)

```
....
121.                            for (i=0; i<=numProgram; i++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1020035&projectid=20028&pathid=29
Status	New

The buffer allocated by <= in gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c at line 81 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-2022-47659-TP.c	gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Line	124	124
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v2.0.0-CVE-2022-47659-TP.c
Method static Bool latm_dmx_sync_frame_bs(GF_BitStream *bs, GF_M4ADecSpecInfo *acfg, u32 *nb_bytes, u8 *buffer, u32 *nb_skipped)

```
....
124.                                    for (j=0; j<=num_lay; j++) {
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Buffer Overflow StrcpyStrcat

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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

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 Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

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
```

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 Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

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

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