vul_files_14 Scan Report

Project Name	vul_files_14
Scan Start	Monday, January 6, 2025 7:59:33 PM
Preset	Checkmarx Default
Scan Time	02h:24m:49s
Lines Of Code Scanned	292838
Files Scanned	120
Report Creation Time	Monday, January 6, 2025 10:49:43 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	6/1000 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

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

Excluded: None

Assigned to

Included: All

Categories

Included:

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

Excluded:

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

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

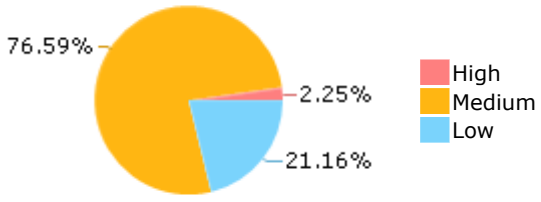
Results Limit

Results limit per query was set to 50

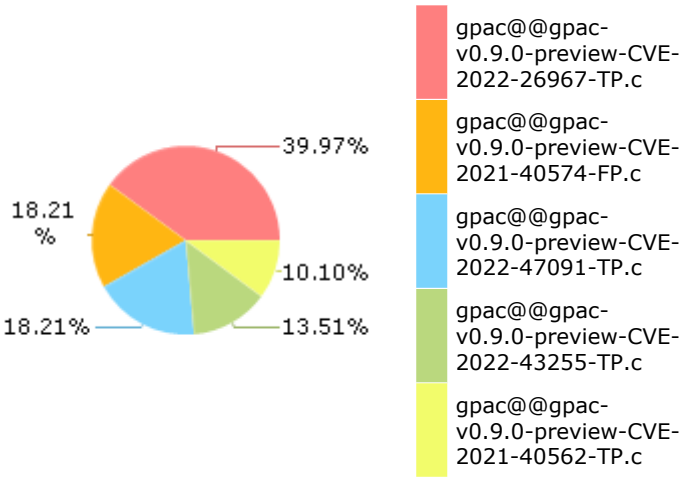
Selected Queries

Selected queries are listed in Result Summary

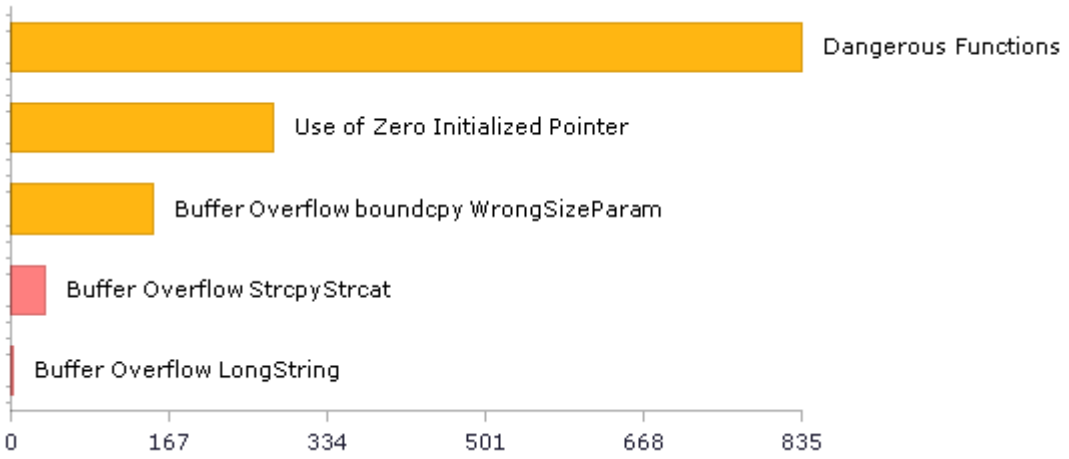
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

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

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	295	244
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	74	74
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	4	4
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	835	835
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	835	835
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	3	3
PCI DSS (3.2) - 6.5.2 - Buffer overflows	211	190
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.	74	74
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.	4	4
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.	22	22

***** 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)	74	74
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)	4	4
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	332	79
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	160	139
SI-11 Error Handling (P2)*	106	106
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	3	3

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

Scan Summary - OWASP Mobile Top 10 2016

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

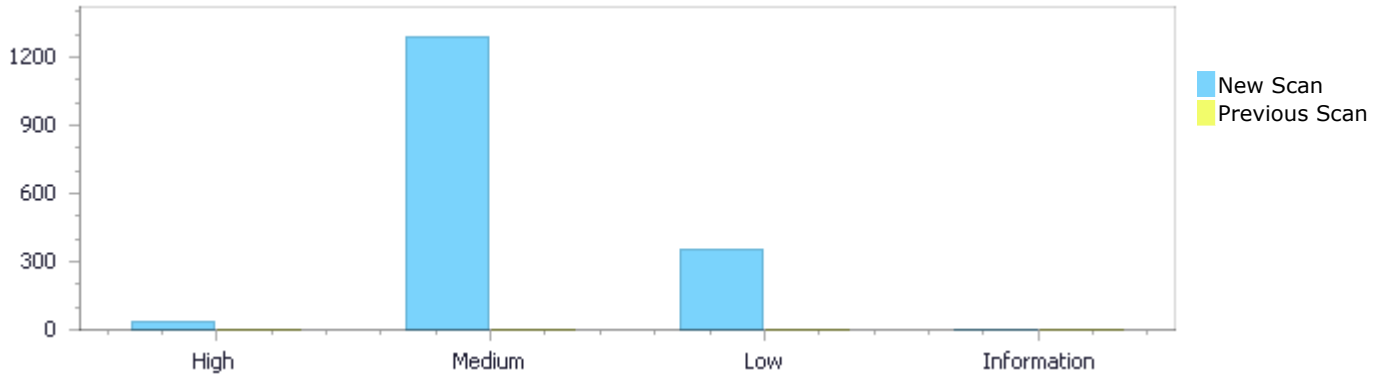
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms,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

Scan Summary - Custom

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

Results Distribution By Status First scan of the project

	High	Medium	Low	Information	Total
New Issues	38	1,292	357	0	1,687
Recurrent Issues	0	0	0	0	0
Total	38	1,292	357	0	1,687
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	38	1,292	357	0	1,687
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	38	1,292	357	0	1,687

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	36	High
Buffer Overflow LongString	2	High
Dangerous Functions	835	Medium
Use of Zero Initialized Pointer	276	Medium
Buffer Overflow boundcpy WrongSizeParam	151	Medium

Integer Overflow	22	Medium
Divide By Zero	6	Medium
Memory Leak	2	Medium
Unchecked Return Value	106	Low
Improper Resource Access Authorization	74	Low
NULL Pointer Dereference	54	Low
Unchecked Array Index	51	Low
Potential Precision Problem	49	Low
Use of Sizeof On a Pointer Type	15	Low
Use of Insufficiently Random Values	4	Low
Potential Off by One Error in Loops	3	Low
Inconsistent Implementations	1	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	168
gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	118
gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	118
gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	82
gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	62
gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	62
gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	62
gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	62
gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	62
gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c	37

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=1000021&projectid=16&pathid=3
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3481
Object	mpd_src	item_path

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void revert_cache_file(char *item_path)

```
....
3481.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=4
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3481
Object	output_dir	item_path

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

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

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

Method static void revert_cache_file(char *item_path)

```
....
3481.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=5
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3468	3481
Object	item_path	item_path

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

Method static void revert_cache_file(char *item_path)

```
....
3468.  static void revert_cache_file(char *item_path)
....
3481.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=6
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3482
Object	mpd_src	szPATH

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

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

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

Method static void revert_cache_file(char *item_path)

```
....
3482.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=7
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3482
Object	output_dir	szPATH

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void revert_cache_file(char *item_path)

```
....
3482.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=8
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3468 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3468	3482
Object	item_path	szPATH

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void revert_cache_file(char *item_path)

```
....
3468.  static void revert_cache_file(char *item_path)
....
3482.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=9
Status	New

The size of the buffer used by rip_mpd in sess, at line 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3565
Object	mpd_src	sess

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3565.       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=1000021&projectid=16&pathid=10
Status	New

The size of the buffer used by rip_mpd in gf_dm_sess_get_cache_name, at line 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3565
Object	mpd_src	gf_dm_sess_get_cache_name

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3565.       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=1000021&projectid=16&pathid=11
Status	New

The size of the buffer used by rip_mpd in output_dir, at line 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3541
Object	output_dir	output_dir

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3541.            strcpy(szName, output_dir);
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=12
Status	New

The size of the buffer used by rip_mpd in szName, at line 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3525	3565
Object	output_dir	szName

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3565.       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=1000021&projectid=16&pathid=13
Status New

The size of the buffer used by revert_cache_file in item_path, at line 3468 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3481
Object	mpd_src	item_path

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

```
....
3481.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=14
Status New

The size of the buffer used by revert_cache_file in item_path, at line 3468 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3481
Object	output_dir	item_path

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

```
....
3481.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=15
Status	New

The size of the buffer used by revert_cache_file in item_path, at line 3468 of gpac@@gpac-v0.9.0-preview-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 3468 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3468	3481
Object	item_path	item_path

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

```
....
3468.  static void revert_cache_file(char *item_path)
....
3481.       strcpy(szPATH, item_path);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=16
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 3468 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3482
Object	mpd_src	szPATH

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c

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

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c

Method static void revert_cache_file(char *item_path)

```
....
3482.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=17
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 3468 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3482
Object	output_dir	szPATH

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
```

File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

```
....
3482.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=18
Status	New

The size of the buffer used by revert_cache_file in szPATH, at line 3468 of gpac@@gpac-v0.9.0-preview-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 3468 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3468	3482
Object	item_path	szPATH

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method static void revert_cache_file(char *item_path)

```
....
3468.  static void revert_cache_file(char *item_path)
....
3482.       strcat(szPATH, ".txt");
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=19
Status	New

The size of the buffer used by rip_mpd in sess, at line 3525 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3565
Object	mpd_src	sess

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3565.       strcpy(szName, gf_dm_sess_get_cache_name(sess) );
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=20
Status	New

The size of the buffer used by rip_mpd in gf_dm_sess_get_cache_name, at line 3525 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3565
Object	mpd_src	gf_dm_sess_get_cache_name

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3565.       strcpy(szName, gf_dm_sess_get_cache_name(sess) );
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=21
Status	New

The size of the buffer used by rip_mpd in output_dir, at line 3525 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3541
Object	output_dir	output_dir

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3541.            strcpy(szName, output_dir);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=22
Status	New

The size of the buffer used by rip_mpd in szName, at line 3525 of gpac@@gpac-v0.9.0-preview-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 3525 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3525	3565
Object	output_dir	szName

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method	GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3525.  GF_Err rip_mpd(const char *mpd_src, const char *output_dir)
....
3565.       strcpy(szName, gf_dm_sess_get_cache_name(sess) );
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=23
Status	New

The size of the buffer used by gf_dump_to_vobsub in szName, at line 226 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_dump_to_vobsub passes to szName, at line 226 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	226	242
Object	szName	szName

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method	static GF_Err gf_dump_to_vobsub(GF_MediaExporter *dumper, char *szName, u32 track, char *dsi, u32 dsiSize)

```
....
226.  static GF_Err gf_dump_to_vobsub(GF_MediaExporter *dumper, char
*szName, u32 track, char *dsi, u32 dsiSize)
....
242.              strcpy(szPath, szName);
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=24
Status	New

The size of the buffer used by gf_dump_to_vobsub in szName, at line 226 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_dump_to_vobsub passes to szName, at line 226 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	226	257
Object	szName	szName

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_dump_to_vobsub(GF_MediaExporter *dumper, char *szName, u32 track, char *dsi, u32 dsiSize)

```
....
226.  static GF_Err gf_dump_to_vobsub(GF_MediaExporter *dumper, char
*szName, u32 track, char *dsi, u32 dsiSize)
....
257.        szName = strcat(szName, ".sub");
```

Buffer Overflow StrcpyStrcat\Path 23:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=25
Status New

The size of the buffer used by gf_dump_to_vobsub in szPath, at line 226 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_dump_to_vobsub passes to szName, at line 226 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	226	243
Object	szName	szPath

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_dump_to_vobsub(GF_MediaExporter *dumper, char *szName, u32 track, char *dsi, u32 dsiSize)

```
....
226.  static GF_Err gf_dump_to_vobsub(GF_MediaExporter *dumper, char
*szName, u32 track, char *dsi, u32 dsiSize)
....
243.              strcat(szPath, ".idx");
```

Buffer Overflow StrcpyStrcat\Path 24:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=26
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_text_get_utf8_line passes to szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	228	306
Object	szLine	szLine

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

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

Buffer Overflow StrcpyStrcat\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=27
Status	New

The size of the buffer used by SFS_AddString in string, at line 70 of gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that SFS_AddString passes to str, at line 70 of gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	70	81
Object	str	string

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
70.  static void SFS_AddString(ScriptParser *parser, char *str)
....
81.   strcat(parser->string, str);
```

Buffer Overflow StrcpyStrcat\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=28
Status	New

The size of the buffer used by SFS_AddString in string, at line 70 of gpac@@gpac-v0.9.0-preview-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_AddString passes to str, at line 70 of gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Line	70	81
Object	str	string

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
70.  static void SFS_AddString(ScriptParser *parser, char *str)
....
81.   strcat(parser->string, str);
```

Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=29
Status	New

The size of the buffer used by xmt_parse_url in vals, at line 824 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	757	844
Object	name	vals

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-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 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=30
Status	New

The size of the buffer used by xmt_parse_url in vals, at line 824 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	824	844
Object	name	vals

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 29:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=31
Status	New

The size of the buffer used by xmt_strip_name in in, at line 1242 of gpac@@gpac-v0.9.0-preview-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 1242 of gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	1242	1245
Object	in	in

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Method static void xmt_strip_name(const char *in, char *out)

```
....
1242.  static void xmt_strip_name(const char *in, char *out)
....
1245.        strcpy(out, in);
```

Buffer Overflow StrcpyStrcat\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=32
Status	New

The size of the buffer used by xmt_strip_name in out, at line 1242 of gpac@@gpac-v0.9.0-preview-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 1242 of gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	1242	1245
Object	out	out

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Method static void xmt_strip_name(const char *in, char *out)

```
....
1242.  static void xmt_strip_name(const char *in, char *out)
....
1245.        strcpy(out, in);
```

Buffer Overflow StrcpyStrcat\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=33
Status	New

The size of the buffer used by *gf_text_get_utf8_line in szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *gf_text_get_utf8_line passes to szLine, at line 228 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	228	306
Object	szLine	szLine

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

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

Buffer Overflow StrcpyStrcat\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=34
Status	New

The size of the buffer used by ephy_string_shorten in new_str, at line 93 of GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ephy_string_shorten passes to str, at line 93 of GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c, to overwrite the target buffer.

	Source	Destination
File	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Line	93	122
Object	str	new_str

Code Snippet
File Name GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c

Method	ephy_string_shorten (char *str,

```
....
93.  ephy_string_shorten (char  *str,
....
122.    strcat (new_str, "…");
```

Buffer Overflow StrcpyStrcat\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=35
Status	New

The size of the buffer used by ephy_string_shorten in new_str, at line 93 of GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ephy_string_shorten passes to str, at line 93 of GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c, to overwrite the target buffer.

	Source	Destination
File	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Line	93	122
Object	str	new_str

Code Snippet	
File Name	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Method	ephy_string_shorten (char *str,

```
....
93.  ephy_string_shorten (char  *str,
....
122.    strcat (new_str, "…");
```

Buffer Overflow StrcpyStrcat\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=36
Status	New

The size of the buffer used by ephy_string_shorten in new_str, at line 93 of GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ephy_string_shorten passes to str, at line 93 of GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c, to overwrite the target buffer.

	Source	Destination
File	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Line	93	122

Object	str	new_str

Code Snippet
File Name GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Method ephy_string_shorten (char *str,

```
....
93.  ephy_string_shorten (char  *str,
....
122.    strcat (new_str, "…");
```

Buffer Overflow StrcpyStrcat\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=37
Status	New

The size of the buffer used by ephy_string_shorten in new_str, at line 93 of GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ephy_string_shorten passes to str, at line 93 of GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c, to overwrite the target buffer.

	Source	Destination
File	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Line	93	122
Object	str	new_str

Code Snippet
File Name GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Method ephy_string_shorten (char *str,

```
....
93.  ephy_string_shorten (char  *str,
....
122.    strcat (new_str, "…");
```

Buffer Overflow StrcpyStrcat\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=38
Status	New

The size of the buffer used by ephy_string_shorten in new_str, at line 93 of GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ephy_string_shorten passes to str, at line 93 of GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c, to overwrite the target buffer.

	Source	Destination
File	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Line	93	122
Object	str	new_str

Code Snippet
File Name GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Method ephy_string_shorten (char *str,

```
....
93.  ephy_string_shorten (char  *str,
....
122.    strcat (new_str, "…");
```

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=1000021&projectid=16&pathid=1
Status	New

The size of the buffer used by SFS_AddChar in msg, at line 90 of gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.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-v0.9.0-preview-CVE-2022-24578-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	93	94
Object	"%c"	msg

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Method static void SFS_AddChar(ScriptParser *parser, char c)

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

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=2
Status	New

The size of the buffer used by SFS_AddChar in msg, at line 90 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-3222-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Line	93	94
Object	"%c"	msg

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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=1000021&projectid=16&pathid=218
Status	New

The dangerous function, memcpy, was found in use at line 350 in GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	584	584
Object	memcpy	memcpy

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
584.                memcpy (&tmp.col[y * tmp.width * 3 + x * 3],
```

Dangerous Functions\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=219
Status New

The dangerous function, memcpy, was found in use at line 350 in GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	584	584
Object	memcpy	memcpy

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
584.                memcpy (&tmp.col[y * tmp.width * 3 + x * 3],
```

Dangerous Functions\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=220
Status New

The dangerous function, memcpy, was found in use at line 715 in gpac@@gpac-v0.9.0-preview-CVE-2021-30015-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-v0.9.0-preview-CVE-2021-30015-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Line	734	734
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Method static GF_Err av1dmx_parse_flush_sample(GF_Filter *filter, GF_AV1DmxCtx *ctx)

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

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=221
Status	New

The dangerous function, memcpy, was found in use at line 867 in gpac@@gpac-v0.9.0-preview-CVE-2021-30015-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-v0.9.0-preview-CVE-2021-30015-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Line	930	930
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=222
Status	New

The dangerous function, memcpy, was found in use at line 867 in gpac@@gpac-v0.9.0-preview-CVE-2021-30015-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-v0.9.0-preview-CVE-2021-30015-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Line	962	962
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=223
Status New

The dangerous function, memcpy, was found in use at line 867 in gpac@@gpac-v0.9.0-preview-CVE-2021-30015-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-v0.9.0-preview-CVE-2021-30015-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Line	980	980
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Method GF_Err av1dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=224

Status	New

The dangerous function, memcpy, was found in use at line 476 in gpac@@gpac-v0.9.0-preview-CVE-2021-30019-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-v0.9.0-preview-CVE-2021-30019-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Line	530	530
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=225
Status	New

The dangerous function, memcpy, was found in use at line 476 in gpac@@gpac-v0.9.0-preview-CVE-2021-30019-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-v0.9.0-preview-CVE-2021-30019-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Line	649	649
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Method GF_Err adts_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=226
Status	New

The dangerous function, memcpy, was found in use at line 421 in gpac@@gpac-v0.9.0-preview-CVE-2021-30199-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-v0.9.0-preview-CVE-2021-30199-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Line	465	465
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=227
Status	New

The dangerous function, memcpy, was found in use at line 421 in gpac@@gpac-v0.9.0-preview-CVE-2021-30199-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-v0.9.0-preview-CVE-2021-30199-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Line	508	508
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Method GF_Err latm_dmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 11:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=228
Status	New

The dangerous function, memcpy, was found in use at line 144 in gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2021-32134-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Line	266	266
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Method GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
266.                    memcpy(esd->decoderConfig->decoderSpecificInfo->data, vtte->config->string, esd->decoderConfig->decoderSpecificInfo->dataLength);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=229
Status	New

The dangerous function, memcpy, was found in use at line 144 in gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2021-32134-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Line	340	340
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Method GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
340.                    memcpy(esd->decoderConfig->decoderSpecificInfo-
>data, ptr->lsr_config->hdr, sizeof(char)*ptr->lsr_config->hdr_size);
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=230
Status	New

The dangerous function, memcpy, was found in use at line 144 in gpac@@gpac-v0.9.0-preview-CVE-2021-32137-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-v0.9.0-preview-CVE-2021-32137-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c
Line	266	266
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c
Method GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
266.                    memcpy(esd->decoderConfig->decoderSpecificInfo-
>data, vtte->config->string, esd->decoderConfig->decoderSpecificInfo-
>dataLength);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=231
Status	New

The dangerous function, memcpy, was found in use at line 144 in gpac@@gpac-v0.9.0-preview-CVE-2021-32137-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-v0.9.0-preview-CVE-2021-32137-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c
Line	340	340
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c
Method	GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
340.                    memcpy(esd->decoderConfig->decoderSpecificInfo->data, ptr->lsr_config->hdr, sizeof(char)*ptr->lsr_config->hdr_size);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=232
Status	New

The dangerous function, memcpy, was found in use at line 523 in gpac@@gpac-v0.9.0-preview-CVE-2021-33363-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-v0.9.0-preview-CVE-2021-33363-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-33363-FP.c
Line	548	548
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-33363-FP.c
Method	GF_Err infe_box_read(GF_Box *s, GF_BitStream *bs)

```
....
548.                            memcpy(ptr->item_name, buf+string_start, string_len);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=233
Status	New

The dangerous function, memcpy, was found in use at line 523 in gpac@@gpac-v0.9.0-preview-CVE-2021-33363-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-v0.9.0-preview-CVE-2021-	gpac@@gpac-v0.9.0-preview-CVE-2021-

	33363-FP.c	33363-FP.c
Line	551	551
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-33363-FP.c
Method GF_Err infe_box_read(GF_Box *s, GF_BitStream *bs)

```
....
551.                            memcpy(ptr->content_type,
buf+string_start, string_len);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=234
Status	New

The dangerous function, memcpy, was found in use at line 523 in gpac@@gpac-v0.9.0-preview-CVE-2021-33363-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-v0.9.0-preview-CVE-2021-33363-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-33363-FP.c
Line	554	554
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-33363-FP.c
Method GF_Err infe_box_read(GF_Box *s, GF_BitStream *bs)

```
....
554.                            memcpy(ptr->content_encoding,
buf+string_start, string_len);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=235
Status	New

The dangerous function, memcpy, was found in use at line 1315 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

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

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=236
Status	New

The dangerous function, memcpy, was found in use at line 1315 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	1397	1397
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

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

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=237
Status	New

The dangerous function, memcpy, was found in use at line 1593 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	1661	1661
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static s32 naludmx_parse_nal_hevc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=238
Status New

The dangerous function, memcpy, was found in use at line 1593 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	1722	1722
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static s32 naludmx_parse_nal_hevc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 22:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=239
Status	New

The dangerous function, memcpy, was found in use at line 1752 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	1816	1816
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static s32 naludmx_parse_nal_avc(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 nal_type, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=240
Status	New

The dangerous function, memcpy, was found in use at line 1752 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	1840	1840
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static s32 naludmx_parse_nal_avc(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 nal_type, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=241
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2021	2021
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=242
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2101	2101
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=243
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2112	2112
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=244
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2122	2122
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=245
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2217	2217
Object	memcpy	memcpy

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method	GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=246
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2221	2221

Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=247
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2264	2264
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=248
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-	gpac@@gpac-v0.9.0-preview-CVE-2021-

	40562-TP.c	40562-TP.c
Line	2268	2268
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=249
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2369	2369
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=250
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2408	2408
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=251
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2421	2421
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=252
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2468	2468
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=253
Status New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2607	2607
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=254
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2805	2805
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=255
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2814	2814
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 39:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=256
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2823	2823
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=257
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2841	2841
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2841.                   memcpy(pck_data, hdr_start,
nal_bytes_from_store);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=258
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2845	2845
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2845.                           memcpy(pck_data + nal_bytes_from_store,
pck_start, (size_t) size);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=259
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2855	2855
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2855.                    memcpy(pck_data, pck_start, (size_t) size);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=260
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2860	2860
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2860.                        memcpy(ctx->hdr_store, start+remain-3, 3);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=261
Status	New

The dangerous function, memcpy, was found in use at line 1315 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	1387	1387
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c

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

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

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=262
Status	New

The dangerous function, memcpy, was found in use at line 1315 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	1397	1397
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method	static void naludmx_queue_param_set(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 ps_type, s32 ps_id)

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

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=263
Status	New

The dangerous function, memcpy, was found in use at line 1593 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	1661	1661
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method	static s32 naludmx_parse_nal_hevc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=264
Status	New

The dangerous function, memcpy, was found in use at line 1593 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	1722	1722
Object	memcpy	memcpy

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method	static s32 naludmx_parse_nal_hevc(GF_NALUDmxCtx *ctx, char *data, u32 size, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=265
Status	New

The dangerous function, memcpy, was found in use at line 1752 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-	gpac@@gpac-v0.9.0-preview-CVE-2021-

	40563-TP.c	40563-TP.c
Line	1816	1816
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static s32 naludmx_parse_nal_avc(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 nal_type, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=266
Status	New

The dangerous function, memcpy, was found in use at line 1752 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	1840	1840
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static s32 naludmx_parse_nal_avc(GF_NALUDmxCtx *ctx, char *data, u32 size, u32 nal_type, Bool *skip_nal, Bool *is_slice, Bool *is_islice)

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

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=267
Status	New

The dangerous function, memcpy, was found in use at line 1928 in gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	2021	2021
Object	memcpy	memcpy

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

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

Use of Zero Initialized Pointer

Query Path:
CPP\Cx\CPP Medium Threat\Use of Zero Initialized Pointer Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description
Use of Zero Initialized Pointer\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1338
Status	New

The variable declared in group at GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c in line 342 is not initialized when it is used by group at GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c in line 342.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c	GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c
Line	352	473
Object	group	group

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c
Method gimp_color_select_init (GimpColorSelect *select)

```
....
352.    GSList                  *group = NULL;
....
473.                group = gtk_radio_button_get_group (GTK_RADIO_BUTTON
(button));
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1339
Status	New

The variable declared in profile at GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c in line 1961 is not initialized when it is used by transform at GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c in line 1961.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c	GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c
Line	1965	1972
Object	profile	transform

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_20-CVE-2022-0520-FP.c
Method gimp_color_select_create_transform (GimpColorSelect *select)

```
....
1965.         static GimpColorProfile *profile = NULL;
....
1972.         select->transform = gimp_widget_get_color_transform
(GTK_WIDGET (select),
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1340
Status	New

The variable declared in xpos at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by xpos at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	368	837
Object	xpos	xpos

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
368.    int         *xpos = NULL, *ypos = NULL;
....
837.            b = xpos[j]; xpos[j] = xpos[a]; xpos[a] = b;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1341
Status	New

The variable declared in xpos at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by xpos at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	368	837
Object	xpos	xpos

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
368.    int         *xpos = NULL, *ypos = NULL;
....
837.            b = xpos[j]; xpos[j] = xpos[a]; xpos[a] = b;
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1342
Status	New

The variable declared in xpos at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by xpos at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	368	875
Object	xpos	xpos

Code Snippet

File Name	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method	repaint (ppm_t *p, ppm_t *a)

```
....
368.    int         *xpos = NULL, *ypos = NULL;
....
875.            tx = xpos[i - 1];
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1343
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1137	1154
Object	col	col

Code Snippet

File Name	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method	repaint (ppm_t *p, ppm_t *a)

```
....
1137.            tmp.col = NULL;
....
1154.                  h = (tmp.col[py * tmp.width * 3 + px * 3]-128) *
relief;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1344
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1133	1154

Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1133.            paper_ppm.col = NULL;
....
1154.                  h = (tmp.col[py * tmp.width * 3 + px * 3]-128) *
relief;
```

Use of Zero Initialized Pointer\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1345
Status New

The variable declared in col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1137	1156
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1137.            tmp.col = NULL;
....
1156.                  h = (tmp.col[py * tmp.width * 3 + px * 3] -
```

Use of Zero Initialized Pointer\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1346
Status New

The variable declared in col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1133	1156
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1133.            paper_ppm.col = NULL;
....
1156.                  h = (tmp.col[py * tmp.width * 3 + px * 3] -
```

Use of Zero Initialized Pointer\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1347
Status New

The variable declared in col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1137	1157
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1137.            tmp.col = NULL;
....
1157.                        (int)tmp.col[((py + 1) % tmp.height) *
tmp.width * 3 +
```

Use of Zero Initialized Pointer\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1348
Status New

The variable declared in col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1133	1157
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1133.            paper_ppm.col = NULL;
....
1157.                          (int)tmp.col[((py + 1) % tmp.height) *
tmp.width * 3 +
```

Use of Zero Initialized Pointer\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1349
Status New

The variable declared in arow at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 228 is not initialized when it is used by arow at GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c in line 228.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	294	313
Object	arow	arow

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method apply_brush (ppm_t *brush,

```
....
294.        guchar *arow = NULL;
....
313.                    arow[(tx + x) * 3] *= v;
```

Use of Zero Initialized Pointer\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=1350
Status	New

The variable declared in xpos at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by xpos at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	368	837
Object	xpos	xpos

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
368.    int         *xpos = NULL, *ypos = NULL;
....
837.            b = xpos[j]; xpos[j] = xpos[a]; xpos[a] = b;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1351
Status	New

The variable declared in xpos at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by xpos at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	368	837
Object	xpos	xpos

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
368.    int         *xpos = NULL, *ypos = NULL;
....
837.            b = xpos[j]; xpos[j] = xpos[a]; xpos[a] = b;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1352
Status	New

The variable declared in xpos at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by xpos at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	368	875
Object	xpos	xpos

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
368.    int         *xpos = NULL, *ypos = NULL;
....
875.            tx = xpos[i - 1];
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1353
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1137	1154
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1137.            tmp.col = NULL;
....
1154.                  h = (tmp.col[py * tmp.width * 3 + px * 3]-128) *
relief;
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1354
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1133	1154
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1133.            paper_ppm.col = NULL;
....
1154.                  h = (tmp.col[py * tmp.width * 3 + px * 3]-128) *
relief;
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1355
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1137	1156
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1137.            tmp.col = NULL;
....
1156.                  h = (tmp.col[py * tmp.width * 3 + px * 3] -
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1356
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1133	1156
Object	col	col

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1133.            paper_ppm.col = NULL;
....
1156.                  h = (tmp.col[py * tmp.width * 3 + px * 3] -
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1357
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1137	1157
Object	col	col

Code Snippet

File Name	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method	repaint (ppm_t *p, ppm_t *a)

```
....
1137.            tmp.col = NULL;
....
1157.                        (int)tmp.col[((py + 1) % tmp.height) *
tmp.width * 3 +
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1358
Status	New

The variable declared in col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350 is not initialized when it is used by col at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1133	1157
Object	col	col

Code Snippet

File Name	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method	repaint (ppm_t *p, ppm_t *a)

```
....
1133.            paper_ppm.col = NULL;
....
1157.                        (int)tmp.col[((py + 1) % tmp.height) *
tmp.width * 3 +
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1359
Status	New

The variable declared in arow at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 228 is not initialized when it is used by arow at GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c in line 228.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	294	313

Object	arow	arow

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method apply_brush (ppm_t *brush,

```
....
294.        guchar *arow = NULL;
....
313.                    arow[(tx + x) * 3] *= v;
```

Use of Zero Initialized Pointer\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1360
Status New

The variable declared in metadata at GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c in line 489 is not initialized when it is used by new_metadata at GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c in line 521.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Line	491	532
Object	metadata	new_metadata

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Method gimp_metadata_new (void)

```
....
491.    GimpMetadata *metadata = NULL;
```

File Name GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Method gimp_metadata_duplicate (GimpMetadata *metadata)

```
....
532.        new_metadata = gimp_metadata_deserialize (xml);
```

Use of Zero Initialized Pointer\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1361
Status New

The variable declared in a at gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c in line 104 is not initialized when it is used by a at gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c in line 104.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c
Line	108	127
Object	a	a

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c
Method GF_Err ilst_item_box_read(GF_Box *s,GF_BitStream *bs)

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

Use of Zero Initialized Pointer\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1362
Status New

The variable declared in sgdp at gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c in line 264 is not initialized when it is used by sgdp at gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c in line 264.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c
Line	296	311
Object	sgdp	sgdp

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c
Method GF_Err stbl_SearchSAPs(GF_SampleTableBox *stbl, u32 SampleNumber, GF_ISOSAPType *IsRAP, u32 *prevRAP, u32 *nextRAP)

```
....
296.                    sgdp = NULL;
....
311.                          GF_RollRecoveryEntry *entry =
gf_list_get(sgdp->group_descriptions, sg-
>sample_entries[j].group_description_index - 1);
```

Use of Zero Initialized Pointer\Path 26:

Severity Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1363
Status	New

The variable declared in sgdp at gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c in line 264 is not initialized when it is used by sgdp at gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c in line 264.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c
Line	278	311
Object	sgdp	sgdp

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c
Method GF_Err stbl_SearchSAPs(GF_SampleTableBox *stbl, u32 SampleNumber, GF_ISOSAPType *IsRAP, u32 *prevRAP, u32 *nextRAP)

```
....
278.              GF_SampleGroupDescriptionBox *sgdp = NULL;
....
311.                              GF_RollRecoveryEntry *entry =
gf_list_get(sgdp->group_descriptions, sg-
>sample_entries[j].group_description_index - 1);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1364
Status	New

The variable declared in avc_state at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 309 is not initialized when it is used by avc_state at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 309.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	314	412
Object	avc_state	avc_state

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1365
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	558	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1366
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	552	567
Object	pa	pa

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method	static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1367
Status	New

The variable declared in avc_state at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 309 is not initialized when it is used by avc_state at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 309.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	314	412
Object	avc_state	avc_state

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method	static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1368
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c

Line	558	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1369
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	552	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1370
Status	New

The variable declared in sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c in line 1251 is not initialized when it is used by sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c in line 1251.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c
Line	1263	1268
Object	sub_samples	sub_samples

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

```
....
1263.             sub_samples = NULL;
....
1268.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1371
Status New

The variable declared in sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c in line 1251 is not initialized when it is used by sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c in line 1251.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c
Line	1254	1268
Object	sub_samples	sub_samples

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

```
....
1254.       GF_SubSampleInformationBox *sub_samples=NULL;
....
1268.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1372

Status	New

The variable declared in sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c in line 1251 is not initialized when it is used by sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c in line 1251.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c
Line	1263	1268
Object	sub_samples	sub_samples

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

```
....
1263.             sub_samples = NULL;
....
1268.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1373
Status	New

The variable declared in sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c in line 1251 is not initialized when it is used by sub_samples at gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c in line 1251.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c
Line	1254	1268
Object	sub_samples	sub_samples

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

```
....
1254.       GF_SubSampleInformationBox *sub_samples=NULL;
....
1268.       count = gf_list_count(sub_samples->Samples);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1374
Status	New

The variable declared in fieldValue at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 2005 is not initialized when it is used by buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 757.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	2139	772
Object	fieldValue	buffer

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c

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

```
....
2139.             char *fieldValue = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-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 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1375
Status	New

The variable declared in fieldValue at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 2005 is not initialized when it is used by buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 757.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	2139	793
Object	fieldValue	buffer

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2139.             char *fieldValue = NULL;
```

File Name gpac@@gpac-v0.9.0-preview-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 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1376
Status	New

The variable declared in buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 859 is not initialized when it is used by buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	865	870
Object	buffer	buffer

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1377

Status	New

The variable declared in buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 757 is not initialized when it is used by buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	818	870
Object	buffer	buffer

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-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 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1378
Status	New

The variable declared in buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 757 is not initialized when it is used by buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	792	870
Object	buffer	buffer

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-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 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1379
Status	New

The variable declared in buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 757 is not initialized when it is used by buffer at gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c in line 859.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	771	870
Object	buffer	buffer

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-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 43:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1380
Status	New

The variable declared in avc_state at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 309 is not initialized when it is used by avc_state at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 309.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	314	412
Object	avc_state	avc_state

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1381
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	558	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1382
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	552	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1383
Status	New

The variable declared in avc_state at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 309 is not initialized when it is used by avc_state at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 309.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	314	412
Object	avc_state	avc_state

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1384
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	558	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1385
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	552	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

Use of Zero Initialized Pointer\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1386
Status New

The variable declared in avc_state at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 309 is not initialized when it is used by avc_state at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 309.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Line	314	412
Object	avc_state	avc_state

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method static void naludmx_check_dur(GF_Filter *filter, GF_NALUDmxCtx *ctx)

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

Use of Zero Initialized Pointer\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1387
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 550 is not initialized when it is used by pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c

Line	558	567
Object	pa	pa

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

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=1000021&projectid=16&pathid=45
Status	New

The size of the buffer used by isor_reader_get_sample in bin128, at line 200 of gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that isor_reader_get_sample passes to bin128, at line 200 of gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c
Line	483	483
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c
Method void isor_reader_get_sample(ISOMChannel *ch)

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

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=46
Status	New

The size of the buffer used by BM_ParseIndexInsert in GF_FieldInfo, at line 444 of gpac@@gpac-v0.9.0-preview-CVE-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-v0.9.0-preview-CVE-2022-1795-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c
Line	485	485
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=47
Status	New

The size of the buffer used by BM_ParseIndexValueReplace in GF_FieldInfo, at line 732 of gpac@@gpac-v0.9.0-preview-CVE-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-v0.9.0-preview-CVE-2022-1795-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c
Line	783	783
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=48
Status	New

The size of the buffer used by BM_ParseIndexInsert in GF_FieldInfo, at line 444 of gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BM_ParseIndexInsert passes to GF_FieldInfo, at line 444 of gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c
Line	485	485
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.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 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=49
Status	New

The size of the buffer used by BM_ParseIndexValueReplace in GF_FieldInfo, at line 732 of gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that BM_ParseIndexValueReplace passes to GF_FieldInfo, at line 732 of gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c
Line	783	783
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.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 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=50
Status	New

The size of the buffer used by dump_mpeg2_ts in GF_M2TS_Dump, at line 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3351	3351
Object	GF_M2TS_Dump	GF_M2TS_Dump

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method	void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3351.       memset(&dumper, 0, sizeof(GF_M2TS_Dump));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=51
Status	New

The size of the buffer used by av1dmx_check_dur in AV1State, at line 240 of gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that av1dmx_check_dur passes to AV1State, at line 240 of gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Line	284	284

Object	AV1State	AV1State

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Method static void av1dmx_check_dur(GF_Filter *filter, GF_AV1DmxCtx *ctx)

```
....
284.        memset(&av1state, 0, sizeof(AV1State));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=52
Status	New

The size of the buffer used by av1dmx_probe_data in AV1State, at line 1002 of gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that av1dmx_probe_data passes to AV1State, at line 1002 of gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Line	1023	1023
Object	AV1State	AV1State

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30015-FP.c
Method static const char * av1dmx_probe_data(const u8 *data, u32 size, GF_FilterProbeScore *score)

```
....
1023.                   memset(&state, 0, sizeof(AV1State));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=53
Status	New

The size of the buffer used by adts_dmx_check_pid in GF_M4ADecSpecInfo, at line 253 of gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that adts_dmx_check_pid passes to GF_M4ADecSpecInfo, at line 253 of gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Line	325	325
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Method static void adts_dmx_check_pid(GF_Filter *filter, GF_ADTSDmxCtx *ctx)

```
....
325.        memset(&acfg, 0, sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=54
Status New

The size of the buffer used by *adts_dmx_probe_data in ADTSHeader, at line 713 of gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *adts_dmx_probe_data passes to ADTSHeader, at line 713 of gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Line	718	718
Object	ADTSHeader	ADTSHeader

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30019-FP.c
Method static const char *adts_dmx_probe_data(const u8 *data, u32 size, GF_FilterProbeScore *score)

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

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=55
Status New

The size of the buffer used by latm_dmx_check_dur in GF_M4ADecSpecInfo, at line 215 of gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that latm_dmx_check_dur passes to

GF_M4ADecSpecInfo, at line 215 of gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Line	243	243
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Method static void latm_dmx_check_dur(GF_Filter *filter, GF_LATMDmxCtx *ctx)

```
....
243.        memset(&acfg, 0, sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=56
Status New

The size of the buffer used by senc_Parse in GF_CENCSampleAuxInfo, at line 1229 of gpac@@gpac-v0.9.0-preview-CVE-2021-31254-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that senc_Parse passes to GF_CENCSampleAuxInfo, at line 1229 of gpac@@gpac-v0.9.0-preview-CVE-2021-31254-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-31254-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-31254-FP.c
Line	1286	1286
Object	GF_CENCSampleAuxInfo	GF_CENCSampleAuxInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-31254-FP.c
Method GF_Err senc_Parse(GF_BitStream *bs, GF_TrackBox *trak, GF_TrackFragmentBox *traf, GF_SampleEncryptionBox *senc)

```
....
1286.            memset(sai, 0, sizeof(GF_CENCSampleAuxInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=57
Status New

The size of the buffer used by Media_GetESD in GF_M4ADecSpecInfo, at line 144 of gpac@@gpac-v0.9.0-preview-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 Media_GetESD passes to GF_M4ADecSpecInfo, at line 144 of gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Line	227	227
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Method GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
227.                                    memset(&aacinfo, 0,
sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=58
Status New

The size of the buffer used by dump_mpeg2_ts in GF_M2TS_Dump, at line 3333 of gpac@@gpac-v0.9.0-preview-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 3333 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3351	3351
Object	GF_M2TS_Dump	GF_M2TS_Dump

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3351.       memset(&dumper, 0, sizeof(GF_M2TS_Dump));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=59
Status	New

The size of the buffer used by Media_GetESD in GF_M4ADecSpecInfo, at line 144 of gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Media_GetESD passes to GF_M4ADecSpecInfo, at line 144 of gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c
Line	227	227
Object	GF_M4ADecSpecInfo	GF_M4ADecSpecInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32137-FP.c
Method GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
227.                                    memset(&aacinfo, 0,
sizeof(GF_M4ADecSpecInfo));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=60
Status	New

The size of the buffer used by gppc_box_read in GF_3GPConfig, at line 48 of gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.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-v0.9.0-preview-CVE-2021-32139-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c
Line	52	52
Object	GF_3GPConfig	GF_3GPConfig

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.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 17:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=61
Status	New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_hevc_set_parall_type passes to HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	577	577
Object	HEVCState	HEVCState

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method	static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

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

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=62
Status	New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_hevc_set_parall_type passes to HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	577	577
Object	HEVCState	HEVCState

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method	static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

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

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=63
Status	New

The size of the buffer used by ttxt_parse_text_box in GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_box passes to GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	1755	1755
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method static void ttxt_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
1755.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=64
Status	New

The size of the buffer used by ttxt_parse_text_style in GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_style passes to GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	1768	1768
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c

Method	static void ttxt_parse_text_style(GF_TXTIn *ctx, GF_XMLNode *n, GF_StyleRecord *style)

```
....
1768.       memset(style, 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=65
Status	New

The size of the buffer used by txtin_setup_ttxt in GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_setup_ttxt passes to GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	1873	1873
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method	static GF_Err txtin_setup_ttxt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1873.                               memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=66
Status	New

The size of the buffer used by tx3g_parse_text_box in GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tx3g_parse_text_box passes to GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	2199	2199

Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method static void tx3g_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
2199.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=67
Status	New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	2351	2351
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2351.                           memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=68
Status	New

The size of the buffer used by txtin_process_texml in GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	2418	2418
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2418.
      memset(&styles[nb_styles], 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=69
Status	New

The size of the buffer used by txtin_process_texml in Marker, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to Marker, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	2535	2535
Object	Marker	Marker

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2535.
      memset(&marks[nb_marks], 0, sizeof(Marker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=70
Status	New

The size of the buffer used by BD_DecMFFieldList in GF_FieldInfo, at line 276 of gpac@@gpac-v0.9.0-preview-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 276 of gpac@@gpac-v0.9.0-preview-CVE-2022-1172-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1172-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1172-TP.c
Line	286	286
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

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

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=71
Status New

The size of the buffer used by BD_DecMFFieldVec in GF_FieldInfo, at line 366 of gpac@@gpac-v0.9.0-preview-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 366 of gpac@@gpac-v0.9.0-preview-CVE-2022-1172-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1172-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1172-TP.c
Line	375	375
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

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

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=72
Status New

The size of the buffer used by gppc_box_read in GF_3GPConfig, at line 48 of gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.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-v0.9.0-preview-CVE-2022-1441-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c
Line	52	52
Object	GF_3GPConfig	GF_3GPConfig

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.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 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=73
Status New

The size of the buffer used by BD_DecMFFieldList in GF_FieldInfo, at line 276 of gpac@@gpac-v0.9.0-preview-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 276 of gpac@@gpac-v0.9.0-preview-CVE-2022-2453-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-2453-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-2453-TP.c
Line	286	286
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

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

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=74
Status	New

The size of the buffer used by BD_DecMFFieldVec in GF_FieldInfo, at line 366 of gpac@@gpac-v0.9.0-preview-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 366 of gpac@@gpac-v0.9.0-preview-CVE-2022-2453-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-2453-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-2453-TP.c
Line	375	375
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

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

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=75
Status	New

The size of the buffer used by *gf_isom_new_movie in GF_ISOFile, at line 620 of gpac@@gpac-v0.9.0-preview-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 620 of gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c
Line	627	627
Object	GF_ISOFile	GF_ISOFile

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c
Method GF_ISOFile *gf_isom_new_movie()

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

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=76
Status	New

The size of the buffer used by BD_DecMFFieldList in GF_FieldInfo, at line 276 of gpac@@gpac-v0.9.0-preview-CVE-2022-43043-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 276 of gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c
Line	286	286
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c

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

```
....
286.        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=1000021&projectid=16&pathid=77
Status	New

The size of the buffer used by BD_DecMFFieldVec in GF_FieldInfo, at line 366 of gpac@@gpac-v0.9.0-preview-CVE-2022-43043-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 366 of gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c
Line	375	375
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43043-TP.c

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

```
....
375.        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=1000021&projectid=16&pathid=78
Status	New

The size of the buffer used by *gf_isom_new_movie in GF_ISOFile, at line 620 of gpac@@gpac-v0.9.0-preview-CVE-2022-43254-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 620 of gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c
Line	627	627
Object	GF_ISOFile	GF_ISOFile

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c
Method GF_ISOFile *gf_isom_new_movie()

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

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=79
Status	New

The size of the buffer used by xmt_locate_stream in XMT_ESDLink, at line 381 of gpac@@gpac-v0.9.0-preview-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_locate_stream passes to XMT_ESDLink, at line 381 of gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	408	408
Object	XMT_ESDLink	XMT_ESDLink

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Method static u32 xmt_locate_stream(GF_XMTParser *parser, char *stream_name)

```
....
408.        memset(esdl, 0, sizeof(XMT_ESDLink));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=80
Status	New

The size of the buffer used by BD_DecMFFieldList in GF_FieldInfo, at line 276 of gpac@@gpac-v0.9.0-preview-CVE-2022-45343-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 276 of gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c
Line	286	286
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c
Method GF_Err BD_DecMFFieldList(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

```
....
286.        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=1000021&projectid=16&pathid=81
Status	New

The size of the buffer used by BD_DecMFFieldVec in GF_FieldInfo, at line 366 of gpac@@gpac-v0.9.0-preview-CVE-2022-45343-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 366 of gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c
Line	375	375
Object	GF_FieldInfo	GF_FieldInfo

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-45343-TP.c
Method GF_Err BD_DecMFFieldVec(GF_BifsDecoder * codec, GF_BitStream *bs, GF_Node *node, GF_FieldInfo *field, Bool is_mem_com)

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

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=82
Status	New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_hevc_set_parall_type passes to HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	577	577
Object	HEVCState	HEVCState

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c

Method static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

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

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=83
Status	New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_hevc_set_parall_type passes to HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	577	577
Object	HEVCState	HEVCState

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method	static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

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

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=84
Status	New

The size of the buffer used by naludmx_hevc_set_parall_type in HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_hevc_set_parall_type passes to HEVCState, at line 570 of gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Line	577	577
Object	HEVCState	HEVCState

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method	static void naludmx_hevc_set_parall_type(GF_NALUDmxCtx *ctx, GF_HEVCConfig *hevc_cfg)

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

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=85
Status	New

The size of the buffer used by ttxt_parse_text_box in GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_box passes to GF_BoxRecord, at line 1751 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

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

	47091-TP.c	47091-TP.c
Line	1755	1755
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static void ttxt_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
1755.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=86
Status	New

The size of the buffer used by ttxt_parse_text_style in GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ttxt_parse_text_style passes to GF_StyleRecord, at line 1764 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	1768	1768
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static void ttxt_parse_text_style(GF_TXTIn *ctx, GF_XMLNode *n, GF_StyleRecord *style)

```
....
1768.       memset(style, 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=87
Status	New

The size of the buffer used by txtin_setup_ttxt in GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_setup_ttxt passes to

GF_TextSampleDescriptor, at line 1787 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	1873	1873
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static GF_Err txtin_setup_ttxt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
1873.                                   memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=88
Status New

The size of the buffer used by tx3g_parse_text_box in GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that tx3g_parse_text_box passes to GF_BoxRecord, at line 2195 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	2199	2199
Object	GF_BoxRecord	GF_BoxRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static void tx3g_parse_text_box(GF_XMLNode *n, GF_BoxRecord *box)

```
....
2199.       memset(box, 0, sizeof(GF_BoxRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=89
Status New

The size of the buffer used by txtin_process_texml in GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_TextSampleDescriptor, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	2351	2351
Object	GF_TextSampleDescriptor	GF_TextSampleDescriptor

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2351.                           memset(&td, 0,
sizeof(GF_TextSampleDescriptor));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=90
Status New

The size of the buffer used by txtin_process_texml in GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to GF_StyleRecord, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	2418	2418
Object	GF_StyleRecord	GF_StyleRecord

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2418.
      memset(&styles[nb_styles], 0, sizeof(GF_StyleRecord));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=91
Status	New

The size of the buffer used by txtin_process_texml in Marker, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that txtin_process_texml passes to Marker, at line 2289 of gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	2535	2535
Object	Marker	Marker

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method static GF_Err txtin_process_texml(GF_Filter *filter, GF_TXTIn *ctx)

```
....
2535.
      memset(&marks[nb_marks], 0, sizeof(Marker));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=92
Status	New

The size of the buffer used by isor_reader_get_sample in bin128, at line 200 of gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that isor_reader_get_sample passes to bin128, at line 200 of gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c
Line	482	482
Object	bin128	bin128

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40592-TP.c
Method void isor_reader_get_sample(ISOMChannel *ch)

```
....
482.                          if (memcmp(ch->KID, KID, sizeof(bin128)))
{
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=93
Status	New

The size of the buffer used by gimp_metadata_deserialize_start_element in ->, at line 566 of GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gimp_metadata_deserialize_start_element passes to ->, at line 566 of GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c, to overwrite the target buffer.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Line	594	594
Object	->	->

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Method gimp_metadata_deserialize_start_element (GMarkupParseContext *context,

```
....
594.        strncpy (parse_data->name, name, sizeof (parse_data->name));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=94
Status	New

The size of the buffer used by Media_GetESD in ptr, at line 144 of gpac@@gpac-v0.9.0-preview-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 Media_GetESD passes to ptr, at line 144 of gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Line	340	340
Object	ptr	ptr

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32134-FP.c
Method GF_Err Media_GetESD(GF_MediaBox *mdia, u32 sampleDescIndex, GF_ESD **out_esd, Bool true_desc_only)

```
....
340.                    memcpy(esd->decoderConfig->decoderSpecificInfo-
>data, ptr->lsr_config->hdr, sizeof(char)*ptr->lsr_config->hdr_size);
```

Integer Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Integer Overflow Version:0

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Integer Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=196
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	798	798
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
798.        i *= density;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=197
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	802	802
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
802.         i = (int)(tmp.width * density / maxbrushwidth) *
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=198
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1015	1015
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1015.            r = r * 255.0 / thissum;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=199
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1016	1016
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1016.            g = g * 255.0 / thissum;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=200
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1017	1017
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1017.            b = b * 255.0 / thissum;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=201
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	881	881
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
881.            tx = tx * (1.0 - z) + tmp.width / 2 * z;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=202
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
882.            ty = ty * (1.0 - z) + tmp.height / 2 * z;
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=203
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1009	1009
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1009.                        r += row[k+0] * v;
```

Integer Overflow\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=204
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1010	1010
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1010.                        g += row[k+1] * v;
```

Integer Overflow\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=205
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	1011	1011
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1011.                        b += row[k+2] * v;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=206
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	798	798
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
798.        i *= density;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=207
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	802	802
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
802.         i = (int)(tmp.width * density / maxbrushwidth) *
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=208
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1015	1015
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1015.            r = r * 255.0 / thissum;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=209
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1016	1016
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1016.            g = g * 255.0 / thissum;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=210
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1017	1017
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1017.            b = b * 255.0 / thissum;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=211
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	881	881
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
881.            tx = tx * (1.0 - z) + tmp.width / 2 * z;
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=212
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	882	882
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
882.            ty = ty * (1.0 - z) + tmp.height / 2 * z;
```

Integer Overflow\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=213
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1009	1009
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1009.                        r += row[k+0] * v;
```

Integer Overflow\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=214
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1010	1010
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1010.                        g += row[k+1] * v;
```

Integer Overflow\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=215
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 350 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	1011	1011
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
1011.                        b += row[k+2] * v;
```

Integer Overflow\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=216
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 127 of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	206	206
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method choose_best_brush (ppm_t *p, ppm_t *a, int tx, int ty,

```
....
206.            best = i;
```

Integer Overflow\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=217
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 127 of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	206	206
Object	AssignExpr	AssignExpr

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method choose_best_brush (ppm_t *p, ppm_t *a, int tx, int ty,

```
....
206.            best = i;
```

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=1000021&projectid=16&pathid=39
Status	New

The application performs an illegal operation in repaint, in GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. In line 350, the program attempts to divide by maxbrushwidth, 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 maxbrushwidth in repaint of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c, at line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	802	802
Object	maxbrushwidth	maxbrushwidth

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
802.        i = (int)(tmp.width * density / maxbrushwidth) *
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=40
Status	New

The application performs an illegal operation in repaint, in GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. In line 350, the program attempts to divide by maxbrushheight, 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 maxbrushheight in repaint of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c, at line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	803	803
Object	maxbrushheight	maxbrushheight

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
803.            (int)(tmp.height * density / maxbrushheight);
```

Divide By Zero\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=41
Status New

The application performs an illegal operation in repaint, in GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c. In line 350, the program attempts to divide by maxbrushwidth, 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 maxbrushwidth in repaint of GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c, at line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	825	825
Object	maxbrushwidth	maxbrushwidth

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
825.            int factor = (int)(tmp.width * density / maxbrushwidth +
0.5);
```

Divide By Zero\Path 4:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=42
Status	New

The application performs an illegal operation in repaint, in GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. In line 350, the program attempts to divide by maxbrushwidth, 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 maxbrushwidth in repaint of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c, at line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	802	802
Object	maxbrushwidth	maxbrushwidth

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
802.         i = (int)(tmp.width * density / maxbrushwidth) *
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=43
Status	New

The application performs an illegal operation in repaint, in GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. In line 350, the program attempts to divide by maxbrushheight, 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 maxbrushheight in repaint of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c, at line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	803	803
Object	maxbrushheight	maxbrushheight

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
803.             (int)(tmp.height * density / maxbrushheight);
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=44
Status	New

The application performs an illegal operation in repaint, in GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c. In line 350, the program attempts to divide by maxbrushwidth, 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 maxbrushwidth in repaint of GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c, at line 350.

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	825	825
Object	maxbrushwidth	maxbrushwidth

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
825.            int factor = (int)(tmp.width * density / maxbrushwidth +
0.5);
```

Memory Leak

Query Path:
CPP\Cx\CPP Medium Threat\Memory Leak Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Memory Leak\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1053
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	243	243
Object	name	name

Code Snippet

File Name	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method	int parse_config(char *filename, bridge_t **bridges)

```
....
243.            if (!(bridge->name = strdup(bridge_name))) {
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1054
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	145	145
Object	bridge	bridge

Code Snippet

File Name	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method	static bridge_t *add_bridge(bridge_t **head)

```
....
145.     if ((bridge = malloc(sizeof(*bridge))) != NULL) {
```

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=1000021&projectid=16&pathid=1060
Status	New

The getstr method calls the snprintf function, at line 130 of GNS3@@ubridge-v0.9.17-CVE-2020-14976-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	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c

Line	134	134
Object	snprintf	snprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static int getstr(dictionary *ubridge_config, const char *section, const char *entry, const char **value)

```
....
134.      snprintf(key, MAX_KEY_SIZE, "%s:%s", section, entry);
```

Unchecked Return Value\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1061
Status New

The dump_mpeg2_ts method calls the sprintf function, at line 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3361	3361
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3361.                   sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1062
Status New

The dump_mpeg2_ts method calls the sprintf function, at line 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3398	3398
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3398.              sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1063
Status	New

The dump_mpeg2_ts method calls the sprintf function, at line 3333 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3361	3361
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3361.                    sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1064
Status	New

The dump_mpeg2_ts method calls the sprintf function, at line 3333 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3398	3398
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3398.              sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

Unchecked Return Value\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1065
Status New

The gf_media_export_filters method calls the sprintf function, at line 1064 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	1266	1266
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_media_export_filters(GF_MediaExporter *dumper)

```
....
1266.                    sprintf(szSubArgs, ":sstart=%d:send=%d", dumper-
>sample_num, dumper->sample_num);
```

Unchecked Return Value\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1066
Status New

The gf_media_export_filters method calls the sprintf function, at line 1064 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	1291	1291
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_media_export_filters(GF_MediaExporter *dumper)

```
....
1291.                    sprintf(szSubArgs, ":nhmlonly:filep=%p", dumper->dump_file);
```

Unchecked Return Value\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1067
Status New

The gf_media_export_filters method calls the sprintf function, at line 1064 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	1329	1329
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_media_export_filters(GF_MediaExporter *dumper)

```
....
1329.              sprintf(szSubArgs, "#PID=%d", dumper->trackID);
```

Unchecked Return Value\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1068

Status	New

The gf_media_export_filters method calls the sprintf function, at line 1064 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	1352	1352
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_media_export_filters(GF_MediaExporter *dumper)

```
....
1352.            sprintf(szSubArgs, ":mov=%p", dumper->file);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1069
Status	New

The gf_media_export_filters method calls the sprintf function, at line 1064 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	1372	1372
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method static GF_Err gf_media_export_filters(GF_MediaExporter *dumper)

```
....
1372.            sprintf(szSubArgs, "PID=%d", dumper->trackID);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=1070
Status	New

The gf_media_export_isom method calls the sprintf function, at line 522 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	548	548
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_isom(GF_MediaExporter *dumper)

```
....
548.                sprintf(szName, "%s%s", dumper->out_name, ext ? ext :
".mp4");
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1071
Status	New

The gf_media_export_webvtt_metadata method calls the sprintf function, at line 595 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	621	621
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_webvtt_metadata(GF_MediaExporter *dumper)

```
....
621.                sprintf(szMedia, "%s.media", dumper->out_name);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1072
Status	New

The gf_media_export_webvtt_metadata method calls the sprintf function, at line 595 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	629	629
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_webvtt_metadata(GF_MediaExporter *dumper)

```
....
629.        sprintf(szName, "%s.vtt", dumper->out_name);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1073
Status	New

The gf_media_export_six method calls the sprintf function, at line 825 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	848	848
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_six(GF_MediaExporter *dumper)

```
....
848.        sprintf(szMedia, "%s.media", dumper->out_name);
```

Unchecked Return Value\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1074
Status	New

The gf_media_export_six method calls the sprintf function, at line 825 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-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-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	855	855
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_six(GF_MediaExporter *dumper)

```
....
855.        sprintf(szName, "%s.six", dumper->out_name);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1075
Status	New

The naludmx_process method calls the sprintf function, at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2890	2890
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx->height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1076
Status	New

The naludmx_process method calls the sprintf function, at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c. However, the code does not check the return value from this function, and thus would not detect runtime errors or other unexpected states.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	2890	2890
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx->height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1077
Status	New

The SFS_AddInt method calls the sprintf function, at line 84 of gpac@@gpac-v0.9.0-preview-CVE-2022-24578-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-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	87	87
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Method static void SFS_AddInt(ScriptParser *parser, s32 val)

```
....
87.    sprintf(msg, "%d", val);
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1078
Status	New

The SFS_AddChar method calls the sprintf function, at line 90 of gpac@@gpac-v0.9.0-preview-CVE-2022-24578-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-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	93	93
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Method static void SFS_AddChar(ScriptParser *parser, char c)

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

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1079
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	344	344
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c

Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
344.                sprintf(nhml, "<?xml version=\"1.0\" encoding=\"UTF-
8\" ?>\n");
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1080
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	350	350
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
350.        sprintf(nhml, "<%s version=\"1.0\" ", ctx->szRootName);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1081
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	354	354
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
354.        NHML_PRINT_UINT(GF_PROP_PID_ID, NULL, "trackID")
```

Unchecked Return Value\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1082
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	355	355
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
355.        NHML_PRINT_UINT(GF_PROP_PID_TIMESCALE, NULL, "timeScale")
```

Unchecked Return Value\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1083
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	359	359
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
359.              sprintf(nhml, "inRootOD=\"yes\" ");
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1084
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	364	364
Object	sprintf	sprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
364.              sprintf(nhml, "streamType=\"%d\"
objectTypeIndication=\"%d\" ", ctx->streamtype, ctx->oti);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1085
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	369	369

Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
369.                    sprintf(nhml, "%s=\"%s\" ", "mediaType",
gf_4cc_to_str(p->value.uint));
```

Unchecked Return Value\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1086
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	372	372
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
372.                    NHML_PRINT_4CC(GF_PROP_PID_ISOM_SUBTYPE,
"mediaSubType", "mediaSubType")
```

Unchecked Return Value\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1087
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-	gpac@@gpac-v0.9.0-preview-CVE-2022-

	26967-TP.c	26967-TP.c
Line	374	374
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
374.                    NHML_PRINT_4CC(GF_PROP_PID_CODECID, NULL,
"codecID")
```

Unchecked Return Value\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1088
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	383	383
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
383.                    sprintf(nhml, "width=\"%d\" height=\"%d\" ",
ctx->w, ctx->h);
```

Unchecked Return Value\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1089
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	391	391
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
391.              sprintf(nhml, "sampleRate=\"%d\" numChannels=\"%d\" ",
ctx->sr, ctx->chan);
```

Unchecked Return Value\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1090
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	393	393
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
393.              sprintf(nhml, "sampleRate=\"%d\" numChannels=\"%d\" ",
ctx->sr, ctx->chan);
```

Unchecked Return Value\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1091
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	396	396
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
396.              sprintf(nhml, "bitsPerSample=\"%d\" ",
gf_audio_fmt_bit_depth(p->value.uint));
```

Unchecked Return Value\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1092
Status New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	400	400
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
400.        NHML_PRINT_4CC(0, "codec_vendor", "codecVendor")
```

Unchecked Return Value\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1093

Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	401	401
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
401.        NHML_PRINT_UINT(0, "codec_version", "codecVersion")
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1094
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	402	402
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
402.        NHML_PRINT_UINT(0, "codec_revision", "codecRevision")
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=1095
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	403	403
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
403.        NHML_PRINT_STRING(0, "compressor_name", "compressorName")
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1096
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	404	404
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
404.        NHML_PRINT_UINT(0, "temporal_quality", "temporalQuality")
```

Unchecked Return Value\Path 38:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1097
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	405	405
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
405.        NHML_PRINT_UINT(0, "spatial_quality", "spatialQuality")
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1098
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	406	406
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
406.        NHML_PRINT_UINT(0, "hres", "horizontalResolution")
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1099
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	407	407
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
407.        NHML_PRINT_UINT(0, "vres", "verticalResolution")
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1100
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	408	408
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
408.        NHML_PRINT_UINT(GF_PROP_PID_BIT_DEPTH_Y, NULL, "bitDepth")
```

Unchecked Return Value\Path 42:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1101
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	410	410
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
410.        NHML_PRINT_STRING(0, "meta:xmlns", "xml_namespace")
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1102
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	411	411
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
411.        NHML_PRINT_STRING(0, "meta:schemaloc",
"xml_schema_location")
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1103
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	412	412
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
412.        NHML_PRINT_STRING(0, "meta:mime", "mime_type")
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1104
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	414	414
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
414.        NHML_PRINT_STRING(0, "meta:config", "config")
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1105
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	415	415
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
415.        NHML_PRINT_STRING(0, "meta:aux_mimes", "aux_mime_type")
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1106
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	419	419
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
419.                    sprintf(nhml,
"xmlns=\"http://www.3gpp.org/richmedia\" ");
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1107
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	423	423
Object	sprintf	sprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
423.              NHML_PRINT_UINT(0, "dims:profile", "profile")
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1108
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	424	424
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
424.                NHML_PRINT_UINT(0, "dims:level", "level")
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1109
Status	New

The nhmldump_send_header method calls the sprintf function, at line 332 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	425	425
Object	sprintf	sprintf

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
425.                NHML_PRINT_UINT(0, "dims:pathComponents",
"pathComponents")
```

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=1000021&projectid=16&pathid=1614
Status	New

	Source	Destination

File	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Line	951	951
Object	fprintf	fprintf

Code Snippet
File Name glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
951.          fprintf(stderr, "Failed to initialize GLFW\n");
```

Improper Resource Access Authorization\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1615
Status New

	Source	Destination
File	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Line	989	989
Object	fprintf	fprintf

Code Snippet
File Name glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
989.          fprintf(stderr, "Failed to create GLFW window\n");
```

Improper Resource Access Authorization\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1616
Status New

	Source	Destination
File	glfw@@glfw-3.3.9-CVE-2021-3520-FP.c	glfw@@glfw-3.3.9-CVE-2021-3520-FP.c
Line	67	67
Object	fprintf	fprintf

Code Snippet
File Name glfw@@glfw-3.3.9-CVE-2021-3520-FP.c
Method static void error_callback(int error, const char* description)

```
....
67.      fprintf(stderr, "Error: %s\n", description);
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1617
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	218	218
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method int parse_config(char *filename, bridge_t **bridges)

```
....
218.             fprintf(stderr, "source NIO not found\n");
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1618
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	237	237
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method int parse_config(char *filename, bridge_t **bridges)

```
....
237.             fprintf(stderr, "destination NIO not found\n");
```

Improper Resource Access Authorization\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1619
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	244	244
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method int parse_config(char *filename, bridge_t **bridges)

```
....
244.                fprintf(stderr, "bridge creation: insufficient
memory\n");
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1620
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	52	52
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *create_udp_tunnel(const char *params)

```
....
52.       fprintf(stderr, "invalid UDP tunnel syntax\n");
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1621
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	58	58
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *create_udp_tunnel(const char *params)

```
....
58.      fprintf(stderr, "unable to create UDP NIO\n");
```

Improper Resource Access Authorization\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1622
Status New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	72	72
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *create_unix_socket(const char *params)

```
....
72.       fprintf(stderr, "invalid UNIX domain socket syntax\n");
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1623
Status New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	77	77

Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *create_unix_socket(const char *params)

```
....
77.      fprintf(stderr, "unable to create UNIX NIO\n");
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1624
Status New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	88	88
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *open_ethernet_device(const char *dev_name)

```
....
88.      fprintf(stderr, "unable to open Ethernet device\n");
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1625
Status New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	99	99
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *open_tap_device(const char *dev_name)

```
....
99.      fprintf(stderr, "unable to open TAP device\n");
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1626
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	111	111
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *open_linux_raw(const char *dev_name)

```
....
111.      fprintf(stderr, "unable to open RAW device\n");
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1627
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	124	124
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static nio_t *open_fusion_vmnet(const char *vmnet_name)

```
....
124.      fprintf(stderr, "unable to open Fusion VMnet interface\n");
```

Improper Resource Access Authorization\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1628
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	173	173
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static void parse_filter(dictionary *ubridge_config, const char *bridge_name, bridge_t *bridge)

```
....
173.                fprintf(stderr, "unable to apply filter to source
NIO\n");
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1629
Status	New

	Source	Destination
File	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c	GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Line	177	177
Object	fprintf	fprintf

Code Snippet
File Name GNS3@@ubridge-v0.9.17-CVE-2020-14976-TP.c
Method static void parse_filter(dictionary *ubridge_config, const char *bridge_name, bridge_t *bridge)

```
....
177.                fprintf(stderr, "unable to apply filter to
destination NIO\n");
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=1630
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3559	3559
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3559.       fprintf(stderr, "Downloading %s\n", mpd_src);
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1631
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3652	3652
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3652.                           fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1632
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-	gpac@@gpac-v0.9.0-preview-CVE-2020-

	23932-TP.c	23932-TP.c
Line	3680	3680
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3680.                                   fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1633
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3152	3152
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3152.                       fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1634
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3157	3157

Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3157.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1635
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3165	3165
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3165.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 23:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1636
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3171	3171
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3171.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1637
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3176	3176
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3176.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1638
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3181	3181
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3181.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1639
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3205	3205
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3205.                    fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1640
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3213	3213
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3213.                   fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1641
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3221	3221
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3221.                   fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, prog->pmt_pid);
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1642
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3274	3274
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3274.                           fprintf(dumper->timestamps_info_file,
"%u\t%d\t", pck->stream->pes_start_packet_number, pck->stream->pid);
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1643
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3275	3275
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3275.                           if (interpolated_pcr_value)
fprintf(dumper->timestamps_info_file, "%f",
interpolated_pcr_value/(300.0 * 90000));
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1644
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3276	3276
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3276.                          fprintf(dumper->timestamps_info_file,
"\t");
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1645
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3277	3277
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3277.                          if (pck->DTS) fprintf(dumper-
>timestamps_info_file, "%f", (pck->DTS / 90000.0));
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1646
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3278	3278
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3278.                          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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1647
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3282	3282
Object	fprintf	fprintf

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3282.                              fprintf(dumper-
>timestamps_info_file, "\t%f\n", diff);
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1648
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3283	3283
Object	fprintf	fprintf

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c

Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3283.                                   if (diff<0) fprintf(stderr,
"Warning: detected PTS/DTS value less than current PCR of %g sec\n",
diff);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1649
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3285	3285
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3285.                                   fprintf(dumper-
>timestamps_info_file, "\t\n");
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1650
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3299	3299
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3299.                   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 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1651
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3345	3345
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3345.               fprintf(stderr, "Cannot open %s: no such file\n",
mpeg2ts_file);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1652
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3390	3390
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3390.             fprintf(stderr, "No program number specified,
defaulting to first program\n");
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1653
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3394	3394
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3394.             fprintf(stderr, "No program number nor output filename
specified. No timestamp file will be generated\n");
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1654
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3401	3401
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3401.                   fprintf(stderr, "Cannot open file %s\n",
dumper.timestamps_info_name);
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1655
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3404	3404
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3404.              fprintf(dumper.timestamps_info_file,
"PCK#\tPID\tPCR\tDTS\tPTS\tRAP\tDiscontinuity\tDTS-PCR Diff\n");
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1656
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3450	3450
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void get_file_callback(void *usr_cbk, GF_NETIO_Parameter *parameter)

```
....
3450.                   fprintf(stderr, "download %02d %% at %05d
kpbs\r", (u32) max, bps*8/1000);
```

Improper Resource Access Authorization\Path 44:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1657
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3475	3475
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void revert_cache_file(char *item_path)

```
....
3475.               fprintf(stderr, "%s is not a gpac cache file\n",
item_path);
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1658
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3519	3519
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method static void revert_cache_file(char *item_path)

```
....
3519.               fprintf(stderr, "Failed to reverse %s cache file\n",
item_path);
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1659
Status	New

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3559	3559
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3559.       fprintf(stderr, "Downloading %s\n", mpd_src);
```

Improper Resource Access Authorization\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1660
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3652	3652
Object	fprintf	fprintf

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3652.                           fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1661
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3680	3680
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method	GF_Err rip_mpd(const char *mpd_src, const char *output_dir)

```
....
3680.                                   fprintf(stderr, "Downloading %s\n",
seg_url);
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1662
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3152	3152
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3152.                   fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1663
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3157	3157
Object	fprintf	fprintf

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c

Method	static void on_m2ts_dump_event(GF_M2TS_Demuxer *ts, u32 evt_type, void *par)

```
....
3157.                   fprintf(dumper->timestamps_info_file,
"%u\t%d\n", ts->pck_number, 0);
```

NULL Pointer Dereference

Query Path:
CPP\Cx\CPP Low Visibility\NULL Pointer Dereference Version:1

Categories

NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

NULL Pointer Dereference\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1184
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2020-35980-FP.c in line 1129 is not initialized when it is used by stbl at gpac@@gpac-v0.9.0-preview-CVE-2020-35980-FP.c in line 1129.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-35980-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-35980-FP.c
Line	1162	1191
Object	null	stbl

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-35980-FP.c
Method	GF_Err DoFullInterleave(MovieWriter *mw, GF_List *writers, GF_BitStream *bs, u8 Emulation, u64 StartOffset)

```
....
1162.                   curWriter = NULL;
....
1191.                   if (curWriter->sampleNumber > curWriter->stbl-
>SampleSize->sampleCount) {
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1185
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	558	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1186
Status New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	552	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1187
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	558	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1188
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	552	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1189
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c in line 848 is not initialized when it is used by def_name at gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c in line 848.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c
Line	877	877
Object	null	def_name

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1190
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c in line 848 is not initialized when it is used by def_name at gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c in line 848.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c
Line	877	877
Object	null	def_name

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.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 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1191
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 163.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	179	179
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.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 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1192
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 163.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	179	202
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.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 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1193
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 163 is not initialized when it is used by string at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 70.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	179	81
Object	null	string

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.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-v0.9.0-preview-CVE-2022-24578-FP.c

Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
81.   strcat(parser->string, str);
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1194
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c in line 145.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.c
Line	179	146
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-24578-FP.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-v0.9.0-preview-CVE-2022-24578-FP.c
Method static void SFS_Space(ScriptParser *pars) {

```
....
146.        if (pars->new_line) SFS_AddString(pars, " ");
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1195
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 163.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Line	179	179
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1196
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 163.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Line	179	202
Object	null	new_line

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1197
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by string at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 70.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Line	179	81
Object	null	string

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-3222-TP.c

Method static void SFS_AddString(ScriptParser *parser, char *str)

```
....
81.   strcat(parser->string, str);
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1198
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 163 is not initialized when it is used by new_line at gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c in line 145.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-3222-TP.c
Line	179	146
Object	null	new_line

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-3222-TP.c

Method static void SFS_Space(ScriptParser *pars) {

```
....
146.        if (pars->new_line) SFS_AddString(pars, " ");
```

NULL Pointer Dereference\Path 16:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1199
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	558	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1200
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	552	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1201
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	558	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1202
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	552	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1203
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Line	558	567
Object	null	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1204
Status	New

The variable declared in null at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Line	552	567
Object	null	nalus

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method	static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

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

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1205
Status	New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c in line 538 is not initialized when it is used by r_LastFoundSample at gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c in line 538.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c
Line	577	577
Object	0	r_LastFoundSample

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-31256-FP.c
Method	GF_Err stbl_GetSampleShadow(GF_ShadowSyncBox *stsh, u32 *sampleNumber, u32 *syncNum)

```
....
577.        stsh->r_LastFoundSample = ent ? ent->shadowedSampleNumber :
0;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1206
Status	New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185 is not initialized when it is used by sr at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c

Line	246	246
Object	0	sr

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method GF_Err nhmldump_configure_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_remove)

```
....
246.        ctx->sr = p ? p->value.uint : 0;
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1207
Status	New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185 is not initialized when it is used by chan at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	248	248
Object	0	chan

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method GF_Err nhmldump_configure_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_remove)

```
....
248.        ctx->chan = p ? p->value.uint : 0;
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1208
Status	New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185 is not initialized when it is used by w at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185.

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

	26967-TP.c	26967-TP.c
Line	252	252
Object	0	w

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method GF_Err nhmldump_configure_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_remove)

```
....
252.        ctx->w = p ? p->value.uint : 0;
```

NULL Pointer Dereference\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1209
Status New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185 is not initialized when it is used by h at gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c in line 185.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	254	254
Object	0	h

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method GF_Err nhmldump_configure_pid(GF_Filter *filter, GF_FilterPid *pid, Bool is_remove)

```
....
254.        ctx->h = p ? p->value.uint : 0;
```

NULL Pointer Dereference\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1210
Status New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 402 is not initialized when it is used by Marker at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 402.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c
Line	418	418
Object	0	Marker

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.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 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1211
Status New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 402 is not initialized when it is used by builder at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 402.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c
Line	418	431
Object	0	builder

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.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 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1212
Status New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 402 is not initialized when it is used by rtp_header at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 402.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c
Line	418	431
Object	0	rtp_header

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.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 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1213
Status New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 538 is not initialized when it is used by Marker at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 538.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c
Line	551	551
Object	0	Marker

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.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 31:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1214
Status	New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 538 is not initialized when it is used by rtp_header at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 538.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c
Line	551	568
Object	0	rtp_header

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.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 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1215
Status	New

The variable declared in 0 at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 538 is not initialized when it is used by builder at gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c in line 538.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.c
Line	551	568
Object	0	builder

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-29537-FP.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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1216
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by array_completeness at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	552	562
Object	pa	array_completeness

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
562.              pa->array_completeness = 1;
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1217
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	552	564

Object	pa	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
564.              pa->nalus = gf_list_new();
```

NULL Pointer Dereference\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1218
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	552	563
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
563.              pa->type = nal_type;
```

NULL Pointer Dereference\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1219
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c in line 550.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	552	557
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
557.              if (pa->type == nal_type) break;
```

NULL Pointer Dereference\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1220
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	552	563
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
563.              pa->type = nal_type;
```

NULL Pointer Dereference\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1221
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	552	564
Object	pa	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
564.              pa->nalus = gf_list_new();
```

NULL Pointer Dereference\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1222
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by array_completeness at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	552	562
Object	pa	array_completeness

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
562.              pa->array_completeness = 1;
```

NULL Pointer Dereference\Path 40:

Severity Low
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1223
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	552	557
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
557.              if (pa->type == nal_type) break;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1224
Status	New

The variable declared in pSamp at gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c in line 1173 is not initialized when it is used by sample_delta at gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c in line 1173.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-29340-TP.c
Line	1176	1185
Object	pSamp	sample_delta

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

```
....
1176.       GF_SubSampleInfoEntry *pSamp;
....
1185.             if (last_sample + pSamp->sample_delta > sampleNumber)
return GF_NOT_SUPPORTED;
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1225
Status	New

The variable declared in pSamp at gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c in line 1173 is not initialized when it is used by sample_delta at gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c in line 1173.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43254-TP.c
Line	1176	1185
Object	pSamp	sample_delta

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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)

```
....
1176.       GF_SubSampleInfoEntry *pSamp;
....
1185.             if (last_sample + pSamp->sample_delta > sampleNumber)
return GF_NOT_SUPPORTED;
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1226
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by array_completeness at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

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

	47087-TP.c	47087-TP.c
Line	552	562
Object	pa	array_completeness

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
562.              pa->array_completeness = 1;
```

NULL Pointer Dereference\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1227
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	552	564
Object	pa	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
564.              pa->nalus = gf_list_new();
```

NULL Pointer Dereference\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1228
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	552	563
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
563.              pa->type = nal_type;
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1229
Status New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	552	557
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
557.              if (pa->type == nal_type) break;
```

NULL Pointer Dereference\Path 47:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1230
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by array_completeness at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	552	562
Object	pa	array_completeness

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
562.              pa->array_completeness = 1;
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1231
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by nalus at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	552	564
Object	pa	nalus

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
564.              pa->nalus = gf_list_new();
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1232
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	552	563
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
563.              pa->type = nal_type;
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1233
Status	New

The variable declared in pa at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550 is not initialized when it is used by type at gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c in line 550.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	552	557
Object	pa	type

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method static void naludmx_hevc_add_param(GF_HEVCConfig *cfg, GF_AVCConfigSlot *sl, u8 nal_type)

```
....
552.        GF_HEVCParamArray *pa = NULL;
....
557.              if (pa->type == nal_type) break;
```

Unchecked Array Index

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Array Index Version:1

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Unchecked Array Index\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1287
Status	New

	Source	Destination
File	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Line	341	341
Object	len	len

Code Snippet
File Name GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
341.    new_strv[len] = g_strdup (str);
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1288
Status	New

	Source	Destination
File	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Line	341	341
Object	len	len

Code Snippet
File Name GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
341.    new_strv[len] = g_strdup (str);
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1289
Status New

	Source	Destination
File	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Line	341	341
Object	len	len

Code Snippet
File Name GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
341.    new_strv[len] = g_strdup (str);
```

Unchecked Array Index\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1290
Status New

	Source	Destination
File	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Line	341	341
Object	len	len

Code Snippet
File Name GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
341.    new_strv[len] = g_strdup (str);
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1291
Status	New

	Source	Destination
File	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Line	341	341
Object	len	len

Code Snippet
File Name GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
341.    new_strv[len] = g_strdup (str);
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1292
Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	837	837
Object	a	a

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
837.            b = xpos[j]; xpos[j] = xpos[a]; xpos[a] = b;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1293

Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	838	838
Object	a	a

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
838.            b = ypos[j]; ypos[j] = ypos[a]; ypos[a] = b;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1294
Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Line	286	286
Object	k	k

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method apply_brush (ppm_t *brush,

```
....
286.                    arow[k] *= v;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1295
Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c

Line	319	319
Object	k	k

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_22-CVE-2023-46752-FP.c
Method apply_brush (ppm_t *brush,

```
....
319.            if(img_has_alpha) arow[k] *= v;
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1296
Status New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	837	837
Object	a	a

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method repaint (ppm_t *p, ppm_t *a)

```
....
837.            b = xpos[j]; xpos[j] = xpos[a]; xpos[a] = b;
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1297
Status New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	838	838
Object	a	a

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c

Method	repaint (ppm_t *p, ppm_t *a)

```
....
838.            b = ypos[j]; ypos[j] = ypos[a]; ypos[a] = b;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1298
Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	286	286
Object	k	k

Code Snippet	
File Name	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method	apply_brush (ppm_t *brush,

```
....
286.                    arow[k] *= v;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1299
Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Line	319	319
Object	k	k

Code Snippet	
File Name	GNOME@@gimp-GIMP_2_10_24-CVE-2023-46752-FP.c
Method	apply_brush (ppm_t *brush,

```
....
319.            if(img_has_alpha) arow[k] *= v;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1300
Status	New

	Source	Destination
File	GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c	GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Line	657	657
Object	length	length

Code Snippet
File Name GNOME@@gimp-GIMP_2_10_26-CVE-2023-46752-FP.c
Method gimp_metadata_deserialize_text (GMarkupParseContext *context,

```
....
657.                values[length]     = value;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1301
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c
Line	163	163
Object	dataSize	dataSize

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-19488-FP.c
Method GF_Err ilst_item_box_read(GF_Box *s,GF_BitStream *bs)

```
....
163.              ptr->data->data[ptr->data->dataSize] = 0;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1302
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c
Line	354	354
Object	i	i

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c
Method GF_Err text_box_read(GF_Box *s, GF_BitStream *bs)

```
....
354.                            ptr->textName[i] = c;
```

Unchecked Array Index\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1303
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c
Line	368	368
Object	i	i

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32139-FP.c
Method GF_Err text_box_read(GF_Box *s, GF_BitStream *bs)

```
....
368.                ptr->textName[i] = '\0';                            /*Font
name*/
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1304
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	712	712

Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
712.                            dep->dependent_on_layerID[dep-
>num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1305
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	712	712
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
712.                            dep->dependent_on_layerID[dep-
>num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1306
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	245	245
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c

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

```
....
245.                                szLineConv[j] = 0xc0 | ( (szLine[i]
>> 6) & 0x3 );
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1307
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	251	251
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
251.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1308
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	257	257
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
257.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1309
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	260	260
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
260.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1310
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	266	266
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
266.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1311
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	269	269
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
269.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1312
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	272	272
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
272.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=1313
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	280	280
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
280.                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1314
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	283	283
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
283.                szLineConv[j] = 0;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1315
Status	New

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Line	732	732
Object	alen	alen

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40574-FP.c
Method static GF_Err txtin_process_srt(GF_Filter *filter, GF_TXTIn *ctx)

```
....
732.                                    szLine[alen] = 0;
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1316
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c
Line	354	354
Object	i	i

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c
Method GF_Err text_box_read(GF_Box *s, GF_BitStream *bs)

```
....
354.                                ptr->textName[i] = c;
```

Unchecked Array Index\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1317
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c
Line	368	368
Object	i	i

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-1441-FP.c
Method	GF_Err text_box_read(GF_Box *s, GF_BitStream *bs)

```
....
368.                ptr->textName[i] = '\0';                        /*Font
name*/
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1318
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-1795-TP.c
Line	212	212
Object	count	count

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-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 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1319
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.c
Line	212	212
Object	count	count

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-24575-FP.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 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1320
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	764	764
Object	d_size	d_size

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_frame(GF_NHMLDumpCtx *ctx, char *data, u32 data_size, GF_FilterPacket *pck)

```
....
764.                                ctx->b64_buffer[d_size] = 0;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1321
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	808	808
Object	k	k

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1322
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	814	814
Object	k	k

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1323
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	2410	2410
Object	del_proto_list_size	del_proto_list_size

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Method static void xmt_parse_command(GF_XMTParser *parser, const char *name, const GF_XMLAttribute *attributes, u32 nb_attributes)

```
....
2410.                                   parser->command-
>del_proto_list[parser->command->del_proto_list_size] = p->ID;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1324
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	2501	2501
Object	NbODs	NbODs

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c

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

```
....
2501.                                   odR->OD_ID[odR->NbODs] = od_id;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1325
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	712	712
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet

File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c

Method GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
712.                            dep->dependent_on_layerID[dep-
>num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1326
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	712	712
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
712.                            dep->dependent_on_layerID[dep-
>num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 41:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1327
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Line	712	712
Object	num_layers_dependent_on	num_layers_dependent_on

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method GF_Err naludmx_set_hevc_oinf(GF_NALUDmxCtx *ctx, u8 *max_temporal_id)

```
....
712.                            dep->dependent_on_layerID[dep-
>num_layers_dependent_on] = j;
```

Unchecked Array Index\Path 42:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1328
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c

Line	245	245
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
245.                                szLineConv[j] = 0xc0 | ( (szLine[i]
>> 6) & 0x3 );
```

Unchecked Array Index\Path 43:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1329
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	251	251
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
251.                                szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 44:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1330
Status New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	257	257
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
257.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1331
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	260	260
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
260.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1332
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	266	266
Object	j	j

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method	char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
266.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1333
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	269	269
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
269.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1334
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	272	272
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
272.                                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1335
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	280	280
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
280.                    szLineConv[j] = szLine[i];
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1336
Status	New

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Line	283	283
Object	j	j

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47091-TP.c
Method char *gf_text_get_utf8_line(char *szLine, u32 lineSize, FILE *txt_in, s32 unicode_type)

```
....
283.                szLineConv[j] = 0;
```

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=1000021&projectid=16&pathid=1238
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_%d.raw", at line 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3361	3361
Object	"%s_%d.raw"	"%s_%d.raw"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3361.                    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=1000021&projectid=16&pathid=1239
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_prog_%d_timestamps.txt", at line 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.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 3333 of gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Line	3398	3398
Object	"%s_prog_%d_timestamps.txt"	"%s_prog_%d_timestamps.txt"

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2020-23932-TP.c
Method	void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3398.              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=1000021&projectid=16&pathid=1240
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_%d.raw", at line 3333 of gpac@@gpac-v0.9.0-preview-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 3333 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3361	3361
Object	"%s_%d.raw"	"%s_%d.raw"

Code Snippet

File Name	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method	void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3361.                    sprintf(dumper.dump, "%s_%d.raw", out_name,
dumper.dump_pid);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1241
Status	New

The size of the buffer used by dump_mpeg2_ts in "%s_prog_%d_timestamps.txt", at line 3333 of gpac@@gpac-v0.9.0-preview-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 3333 of gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Line	3398	3398

Object	"%s_prog_%d_timestamps.txt"	"%s_prog_%d_timestamps.txt"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32136-FP.c
Method void dump_mpeg2_ts(char *mpeg2ts_file, char *out_name, Bool prog_num)

```
....
3398.             sprintf(dumper.timestamps_info_name,
"%s_prog_%d_timestamps.txt", mpeg2ts_file, prog_num/*, mpeg2ts_file*/);
```

Potential Precision Problem\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1242
Status New

The size of the buffer used by gf_media_export_isom in "%s%s", at line 522 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_media_export_isom passes to "%s%s", at line 522 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	548	548
Object	"%s%s"	"%s%s"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_isom(GF_MediaExporter *dumper)

```
....
548.             sprintf(szName, "%s%s", dumper->out_name, ext ? ext :
".mp4");
```

Potential Precision Problem\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1243
Status New

The size of the buffer used by gf_media_export_webvtt_metadata in "%s.media", at line 595 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_media_export_webvtt_metadata passes to "%s.media", at line 595 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	621	621
Object	"%s.media"	"%s.media"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_webvtt_metadata(GF_MediaExporter *dumper)

```
....
621.              sprintf(szMedia, "%s.media", dumper->out_name);
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1244
Status	New

The size of the buffer used by gf_media_export_webvtt_metadata in "%s.vtt", at line 595 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_media_export_webvtt_metadata passes to "%s.vtt", at line 595 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	629	629
Object	"%s.vtt"	"%s.vtt"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_webvtt_metadata(GF_MediaExporter *dumper)

```
....
629.          sprintf(szName, "%s.vtt", dumper->out_name);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1245
Status	New

The size of the buffer used by gf_media_export_six in "%s.media", at line 825 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_media_export_six passes to "%s.media", at line 825 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	848	848
Object	"%s.media"	"%s.media"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_six(GF_MediaExporter *dumper)

```
....
848.        sprintf(szMedia, "%s.media", dumper->out_name);
```

Potential Precision Problem\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1246
Status New

The size of the buffer used by gf_media_export_six in "%s.six", at line 825 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gf_media_export_six passes to "%s.six", at line 825 of gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Line	855	855
Object	"%s.six"	"%s.six"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-32438-FP.c
Method GF_Err gf_media_export_six(GF_MediaExporter *dumper)

```
....
855.        sprintf(szName, "%s.six", dumper->out_name);
```

Potential Precision Problem\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1247
Status New

The size of the buffer used by naludmx_process in "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that

naludmx_process passes to "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Line	2890	2890
Object	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40562-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx->height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Potential Precision Problem\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1248
Status New

The size of the buffer used by naludmx_process in "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_process passes to "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Line	2890	2890
Object	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-40563-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx->height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Potential Precision Problem\Path 12:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1249
Status	New

The size of the buffer used by nhmldump_send_header in "<%s version=\"1.0\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "<%s version=\"1.0\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	350	350
Object	"<%s version=\"1.0\" "	"<%s version=\"1.0\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
350.        sprintf(nhml, "<%s version=\"1.0\" ", ctx->szRootName);
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1250
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	354	354
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
354.        NHML_PRINT_UINT(GF_PROP_PID_ID, NULL, "trackID")
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1251
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	355	355
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
355.        NHML_PRINT_UINT(GF_PROP_PID_TIMESCALE, NULL, "timeScale")
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1252
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	369	369
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
369.                    sprintf(nhml, "%s=\"%s\" ", "mediaType",
gf_4cc_to_str(p->value.uint));
```

Potential Precision Problem\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1253
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	372	372
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
372.                    NHML_PRINT_4CC(GF_PROP_PID_ISOM_SUBTYPE,
"mediaSubType", "mediaSubType")
```

Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1254
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	374	374
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
374.                    NHML_PRINT_4CC(GF_PROP_PID_CODECID, NULL,
"codecID")
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1255
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	400	400
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
400.        NHML_PRINT_4CC(0, "codec_vendor", "codecVendor")
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1256
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	401	401

Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
401.        NHML_PRINT_UINT(0, "codec_version", "codecVersion")
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1257
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	402	402
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
402.        NHML_PRINT_UINT(0, "codec_revision", "codecRevision")
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1258
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c

Line	403	403
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
403.        NHML_PRINT_STRING(0, "compressor_name", "compressorName")
```

Potential Precision Problem\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1259
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	404	404
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
404.        NHML_PRINT_UINT(0, "temporal_quality", "temporalQuality")
```

Potential Precision Problem\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1260
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

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

	26967-TP.c	26967-TP.c
Line	405	405
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
405.        NHML_PRINT_UINT(0, "spatial_quality", "spatialQuality")
```

Potential Precision Problem\Path 24:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1261
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	406	406
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
406.        NHML_PRINT_UINT(0, "hres", "horizontalResolution")
```

Potential Precision Problem\Path 25:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1262
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination

File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	407	407
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
407.        NHML_PRINT_UINT(0, "vres", "verticalResolution")
```

Potential Precision Problem\Path 26:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1263
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	408	408
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
408.        NHML_PRINT_UINT(GF_PROP_PID_BIT_DEPTH_Y, NULL, "bitDepth")
```

Potential Precision Problem\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1264
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	410	410
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
410.        NHML_PRINT_STRING(0, "meta:xmlns", "xml_namespace")
```

Potential Precision Problem\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1265
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	411	411
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
411.        NHML_PRINT_STRING(0, "meta:schemaloc",
"xml_schema_location")
```

Potential Precision Problem\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1266
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	412	412
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
412.        NHML_PRINT_STRING(0, "meta:mime", "mime_type")
```

Potential Precision Problem\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1267
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	414	414
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
414.        NHML_PRINT_STRING(0, "meta:config", "config")
```

Potential Precision Problem\Path 31:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1268
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	415	415
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
415.        NHML_PRINT_STRING(0, "meta:aux_mimes", "aux_mime_type")
```

Potential Precision Problem\Path 32:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1269
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	423	423
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
423.              NHML_PRINT_UINT(0, "dims:profile", "profile")
```

Potential Precision Problem\Path 33:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1270
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	424	424
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
424.             NHML_PRINT_UINT(0, "dims:level", "level")
```

Potential Precision Problem\Path 34:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1271
Status New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	425	425
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
425.             NHML_PRINT_UINT(0, "dims:pathComponents",
"pathComponents")
```

Potential Precision Problem\Path 35:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16

	&pathid=1272
Status	New

The size of the buffer used by nhmldump_send_header in "useFullRequestHost=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "useFullRequestHost=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	429	429
Object	"useFullRequestHost=\"%s\" "	"useFullRequestHost=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
429.                    sprintf(nhml, "useFullRequestHost=\"%s\" ", p->value.boolean ? "yes" : "no");
```

Potential Precision Problem\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1273
Status	New

The size of the buffer used by nhmldump_send_header in "stream_type=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "stream_type=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	434	434
Object	"stream_type=\"%s\" "	"stream_type=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
434.                    sprintf(nhml, "stream_type=\"%s\" ", p->value.boolean ? "primary" : "secondary");
```

Potential Precision Problem\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1274
Status	New

The size of the buffer used by nhmldump_send_header in "contains_redundant=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "contains_redundant=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	439	439
Object	"contains_redundant=\"%s\" "	"contains_redundant=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
439.                    sprintf(nhml, "contains_redundant=\"%s\" ", (p->value.uint==1) ? "main" : ((p->value.uint==1) ? "redundant" : "main+redundant") );
```

Potential Precision Problem\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1275
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%d\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	442	442
Object	"%s=\"%d\" "	"%s=\"%d\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
442.              NHML_PRINT_UINT(0, "dims:scriptTypes", "scriptTypes")
```

Potential Precision Problem\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1276
Status	New

The size of the buffer used by nhmldump_send_header in "specificInfoFile=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "specificInfoFile=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	447	447
Object	"specificInfoFile=\"%s\" "	"specificInfoFile=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
447.              sprintf(nhml, "specificInfoFile=\"%s\" ",
gf_file_basename(ctx->info_file) );
```

Potential Precision Problem\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1277
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	456	456
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
456.        NHML_PRINT_STRING(0, "meta:encoding", "encoding")
```

Potential Precision Problem\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1278
Status	New

The size of the buffer used by nhmldump_send_header in "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "%s=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	457	457
Object	"%s=\"%s\" "	"%s=\"%s\" "

Code Snippet	
File Name	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method	static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
457.        NHML_PRINT_STRING(0, "meta:contentEncoding",
"content_encoding")
```

Potential Precision Problem\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1279
Status	New

The size of the buffer used by nhmldump_send_header in "baseMediaFile=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-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 nhmldump_send_header passes to "baseMediaFile=\"%s\" ", at line 332 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c

Line	467	467
Object	"baseMediaFile=\"%s\" "	"baseMediaFile=\"%s\" "

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_send_header(GF_NHMLDumpCtx *ctx)

```
....
467.              sprintf(nhml, "baseMediaFile=\"%s\" ",
gf_file_basename(ctx->media_file) );
```

Potential Precision Problem\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1280
Status	New

The size of the buffer used by nhmldump_pck_property in "%s=\"", at line 602 of gpac@@gpac-v0.9.0-preview-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 nhmldump_pck_property passes to "%s=\"", at line 602 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	609	609
Object	"%s=\""	"%s=\""

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_pck_property(GF_NHMLDumpCtx *ctx, u32 p4cc, const char *pname, const GF_PropertyValue *att)

```
....
609.        sprintf(nhml, "%s=\"", pname ? pname : gf_4cc_to_str(p4cc));
```

Potential Precision Problem\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1281
Status	New

The size of the buffer used by nhmldump_pck_property in "%s", at line 602 of gpac@@gpac-v0.9.0-preview-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 nhmldump_pck_property passes to "%s", at line 602 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	627	627
Object	"%s"	"%s"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method static void nhmldump_pck_property(GF_NHMLDumpCtx *ctx, u32 p4cc, const char *pname, const GF_PropertyValue *att)

```
....
627.              sprintf(nhml, "%s", gf_props_dump_val(att, pval,
GF_FALSE, NULL) );
```

Potential Precision Problem\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1282
Status New

The size of the buffer used by nhmldump_process in "\n", at line 814 of gpac@@gpac-v0.9.0-preview-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 nhmldump_process passes to "\n", at line 814 of gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Line	832	832
Object	"</%s>\n"	"</%s>\n"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-26967-TP.c
Method GF_Err nhmldump_process(GF_Filter *filter)

```
....
832.                          sprintf(nhml, "</%s>\n", ctx->szRootName);
```

Potential Precision Problem\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1283
Status New

The size of the buffer used by xmt_resolve_od_links in "od:%d#%s", at line 427 of gpac@@gpac-v0.9.0-preview-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-v0.9.0-preview-CVE-2022-43255-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-43255-TP.c
Line	585	585
Object	"od:%d#%s"	"od:%d#%s"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-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\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1284
Status New

The size of the buffer used by naludmx_process in "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_process passes to "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Line	2890	2890
Object	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47087-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P %
8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx-
>height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Potential Precision Problem\Path 48:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1285
Status	New

The size of the buffer used by naludmx_process in "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_process passes to "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Line	2890	2890
Object	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47088-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx->height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Potential Precision Problem\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1286
Status	New

The size of the buffer used by naludmx_process in "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that naludmx_process passes to "%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI", at line 1928 of gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c, to overwrite the target buffer.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c	gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Line	2890	2890
Object	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"	"%s %dx%d % 10d NALU % 8d I % 8d P % 8d B % 8d SEI"

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2022-47089-TP.c
Method GF_Err naludmx_process(GF_Filter *filter)

```
....
2890.             sprintf(szStatus, "%s %dx%d % 10d NALU % 8d I % 8d P %
8d B % 8d SEI", ctx->is_hevc ? "HEVC":"AVC|H264", ctx->width, ctx-
>height, ctx->nb_nalus, ctx->nb_i, ctx->nb_p, ctx->nb_b, ctx->nb_sei);
```

Use of Sizeof On a Pointer Type

Query Path:
CPP\Cx\CPP Low Visibility\Use of Sizeof On a Pointer Type Version:1

Description

Use of Sizeof On a Pointer Type\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1166
Status	New

	Source	Destination
File	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Line	226	226
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Method ephy_string_commandline_args_to_uris (char **arguments,

```
....
226.     args = g_malloc0 (sizeof (gchar *) * (g_strv_length (arguments)
+ 1));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1167
Status	New

	Source	Destination
File	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Line	332	332
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
332.    new_strv = g_malloc ((len + 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1168
Status	New

	Source	Destination
File	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Line	361	361
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.35.92-CVE-2022-29536-TP.c
Method ephy_strv_remove (const char * const *strv,

```
....
361.    new_strv = g_malloc ((len - 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1169
Status	New

	Source	Destination
File	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Line	226	226
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Method ephy_string_commandline_args_to_uris (char **arguments,

```
....
226.    args = g_malloc0 (sizeof (gchar *) * (g_strv_length (arguments)
+ 1));
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1170
Status	New

	Source	Destination
File	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Line	332	332
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
332.    new_strv = g_malloc ((len + 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1171
Status	New

	Source	Destination
File	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Line	361	361
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.37.2-CVE-2022-29536-TP.c
Method ephy_strv_remove (const char * const *strv,

```
....
361.    new_strv = g_malloc ((len - 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1172
Status	New

	Source	Destination
File	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Line	226	226
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Method ephy_string_commandline_args_to_uris (char **arguments,

```
....
226.    args = g_malloc0 (sizeof (gchar *) * (g_strv_length (arguments)
+ 1));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1173
Status New

	Source	Destination
File	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Line	332	332
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
332.    new_strv = g_malloc ((len + 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1174
Status New

	Source	Destination
File	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c	GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Line	361	361

Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.37.92-CVE-2022-29536-TP.c
Method ephy_strv_remove (const char * const *strv,

```
....
361.    new_strv = g_malloc ((len - 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1175
Status New

	Source	Destination
File	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Line	226	226
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Method ephy_string_commandline_args_to_uris (char **arguments,

```
....
226.    args = g_malloc0 (sizeof (gchar *) * (g_strv_length (arguments)
+ 1));
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1176
Status New

	Source	Destination
File	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Line	332	332
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
332.    new_strv = g_malloc ((len + 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1177
Status	New

	Source	Destination
File	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Line	361	361
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.38.3-CVE-2022-29536-TP.c
Method ephy_strv_remove (const char * const *strv,

```
....
361.    new_strv = g_malloc ((len - 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1178
Status	New

	Source	Destination
File	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Line	226	226
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Method ephy_string_commandline_args_to_uris (char **arguments,

```
....
226.    args = g_malloc0 (sizeof (gchar *) * (g_strv_length (arguments)
+ 1));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1179
Status	New

	Source	Destination
File	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Line	332	332
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Method ephy_strv_append (const char * const *strv,

```
....
332.    new_strv = g_malloc ((len + 1 + 1) * sizeof (char *));
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1180
Status	New

	Source	Destination
File	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c	GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Line	361	361
Object	sizeof	sizeof

Code Snippet
File Name GNOME@@epiphany-3.38.6-CVE-2022-29536-TP.c
Method ephy_strv_remove (const char * const *strv,

```
....
361.    new_strv = g_malloc ((len - 1 + 1) * sizeof (char *));
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1056
Status	New

Method init_particle at line 244 of glfw@@glfw-3.3.8-CVE-2021-3520-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Line	254	254
Object	rand	rand

Code Snippet
File Name glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Method static void init_particle(PARTICLE *p, double t)

```
....
254.      p->vz = 0.7f + (0.3f / 4096.f) * (float) (rand() & 4095);
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1057
Status	New

Method init_particle at line 244 of glfw@@glfw-3.3.8-CVE-2021-3520-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Line	257	257
Object	rand	rand

Code Snippet
File Name glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Method static void init_particle(PARTICLE *p, double t)

```
....
257.      xy_angle = (2.f * (float) M_PI / 4096.f) * (float) (rand() &
4095);
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1058
Status	New

Method main at line 76 of glfw@@glfw-3.3.9-CVE-2021-3520-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	glfw@@glfw-3.3.9-CVE-2021-3520-FP.c	glfw@@glfw-3.3.9-CVE-2021-3520-FP.c
Line	124	124
Object	rand	rand

Code Snippet
File Name glfw@@glfw-3.3.9-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
124.                    pixels[y * 16 + x] = rand() % 256;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1059
Status	New

Method main at line 76 of glfw@@glfw-3.3.9-CVE-2021-3520-FP.c uses a weak method srand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	glfw@@glfw-3.3.9-CVE-2021-3520-FP.c	glfw@@glfw-3.3.9-CVE-2021-3520-FP.c
Line	119	119
Object	srand	srand

Code Snippet
File Name glfw@@glfw-3.3.9-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
119.            srand((unsigned int) glfwGetTimerValue());
```

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=1000021&projectid=16&pathid=1181
Status	New

The buffer allocated by <= in glfw@@glfw-3.3.8-CVE-2021-3520-FP.c at line 604 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Line	625	625
Object	<=	<=

Code Snippet
File Name glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Method static void draw_fountain(void)

```
....
625.              for (m = 0;  m <= FOUNTAIN_SWEEP_STEPS;  m++)
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1182
Status	New

The buffer allocated by <= in gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c at line 76 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Line	116	116
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Method static Bool latm_dmx_sync_frame_bs(GF_BitStream *bs, GF_M4ADecSpecInfo *acfg, u32 *nb_bytes, u8 *buffer, u32 *nb_skipped)

```
....
116.                            for (i=0; i<=numProgram; i++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1183
Status	New

The buffer allocated by <= in gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c at line 76 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c	gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Line	119	119
Object	<=	<=

Code Snippet
File Name gpac@@gpac-v0.9.0-preview-CVE-2021-30199-FP.c
Method static Bool latm_dmx_sync_frame_bs(GF_BitStream *bs, GF_M4ADecSpecInfo *acfg, u32 *nb_bytes, u8 *buffer, u32 *nb_skipped)

```
....
119.                                    for (j=0; j<=num_lay; j++) {
```

Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

Description

Inconsistent Implementations\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000021&projectid=16&pathid=1055
Status	New

	Source	Destination
File	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c	glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Line	955	955
Object	getopt	getopt

Code Snippet
File Name glfw@@glfw-3.3.8-CVE-2021-3520-FP.c
Method int main(int argc, char** argv)

```
....
955.      while ((ch = getopt(argc, argv, "fh")) != -1)
```

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

Integer Overflow

Risk

What might happen

Assigning large data types into smaller data types, without proper checks and explicit casting, will lead to undefined behavior and unintentional effects, such as data corruption (e.g. value wraparound, wherein maximum values become minimum values); system crashes; infinite loops; logic errors, such as bypassing of security mechanisms; or even buffer overflows leading to arbitrary code execution.

Cause

How does it happen

This flaw can occur when implicitly casting numerical data types of a larger size, into a variable with a data type of a smaller size. This forces the program to discard some bits of information from the number. Depending on how the numerical data types are stored in memory, this is often the bits with the highest value, causing substantial corruption of the stored number. Alternatively, the sign bit of a signed integer could be lost, completely reversing the intention of the number.

General Recommendations

How to avoid it

- Avoid casting larger data types to smaller types.
- Prefer promoting the target variable to a large enough data type.
- If downcasting is necessary, always check that values are valid and in range of the target type, before casting

---

Source Code Examples

CPP

Unsafe Downsize Casting

```
int unsafe_addition(short op1, int op2) {

    // op2 gets forced from int into a short
    short total = op1 + op2;

    return total;
}
```

Safer Use of Proper Data Types

```
int safe_addition(short op1, int op2) {

    // total variable is of type int, the largest type that is needed
    int total = 0;

    // check if total will overflow available integer size
    if (INT_MAX - abs(op2) > op1)
```

```
    {
        total = op1 + op2;
    }
    else
    {
        // instead of overflow, saturate (but this is not always a good thing)
        total = INT_MAX
    }

    return total;
}
```

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;
}
```

Failure to Release Memory Before Removing Last Reference ('Memory Leak')

Weakness ID: 401 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.

Extended Description

This is often triggered by improper handling of malformed data or unexpectedly interrupted sessions.

Terminology Notes

"memory leak" has sometimes been used to describe other kinds of issues, e.g. for information leaks in which the contents of memory are inadvertently leaked (CVE-2003-0400 is one such example of this terminology conflict).

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Modes of Introduction

Memory leaks have two common and sometimes overlapping causes:

- Error conditions and other exceptional circumstances
- Confusion over which part of the program is responsible for freeing the memory

Common Consequences

Scope	Effect
Availability	Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial of service attack (by crashing or hanging the program) or take advantage of other unexpected program behavior resulting from a low memory condition.

Likelihood of Exploit

Medium

Demonstrative Examples

Example 1

The following C function leaks a block of allocated memory if the call to read() fails to return the expected number of bytes:

(Bad Code)

Example Language: **C**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

(Bad Code)

Example Language: **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

Observed Examples

Reference	Description
CVE-2005-3119	Memory leak because function does not free() an element of a data structure.
CVE-2004-0427	Memory leak when counter variable is not decremented.
CVE-2002-0574	Memory leak when counter variable is not decremented.
CVE-2005-3181	Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code.
CVE-2004-0222	Memory leak via unknown manipulations as part of protocol test suite.
CVE-2001-0136	Memory leak via a series of the same command.

Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

Phase: Architecture and Design

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	730	OWASP Top Ten 2004 Category A9 - Denial of Service	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Weakness Base	772	Missing Release of Resource after Effective	**Research Concepts (primary)1000**

			Lifetime	
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
CanFollow	Weakness Class	390	Detection of Error Condition Without Action	Research Concepts1000

Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

Affected Resources

- Memory

Functional Areas

- Memory management

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			Memory leak
7 Pernicious Kingdoms			Memory Leak
CLASP			Failure to deallocate data
OWASP Top Ten 2004	A9	CWE More Specific	Denial of Service

White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	PLOVER		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Other Notes		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-07-17	KDM Analytics		External
	Improved the White Box Definition		

2009-07-27	CWE Content Team	MITRE	Internal
	updated White Box Definitions		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Modes of Introduction, Other Notes		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Memory Leak
2009-05-27	Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak')

BACK TO TOP

Use of 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());
```

Use of Function with Inconsistent Implementations

Weakness ID: 474 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C: *(Often)*

PHP: *(Often)*

All

Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	589	Call to Non-ubiquitous API	**Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Inconsistent Implementations

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 Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Inconsistent Implementations		

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

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
```

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
```

```
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");
```

```
try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Improper Access Control (Authorization)

Weakness ID: 285 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software does not perform or incorrectly performs access control checks across all potential execution paths.

Extended Description

When access control checks are not applied consistently - or not at all - users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information leaks, denial of service, and arbitrary code execution.

Alternate Terms

AuthZ:	"AuthZ" is typically used as an abbreviation of "authorization" within the web application security community. It is also distinct from "AuthC," which is an abbreviation of "authentication." The use of "Auth" as an abbreviation is discouraged, since it could be used for either authentication or authorization.

Time of Introduction

- Architecture and Design
- Implementation
- Operation

Applicable Platforms

Languages

Language-independent

Technology Classes

Web-Server: *(Often)*

Database-Server: *(Often)*

Modes of Introduction

A developer may introduce authorization weaknesses because of a lack of understanding about the underlying technologies. For example, a developer may assume that attackers cannot modify certain inputs such as headers or cookies.

Authorization weaknesses may arise when a single-user application is ported to a multi-user environment.

Common Consequences

Scope	Effect
Confidentiality	An attacker could read sensitive data, either by reading the data directly from a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to read the data.
Integrity	An attacker could modify sensitive data, either by writing the data directly to a data store that is not properly restricted, or by accessing insufficiently-protected, privileged functionality to write the data.
Integrity	An attacker could gain privileges by modifying or reading critical data directly, or by accessing insufficiently-protected, privileged functionality.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

Automated static analysis is useful for detecting commonly-used idioms for authorization. A tool may be able to analyze related configuration files, such as .htaccess in Apache web servers, or detect the usage of commonly-used authorization libraries.

Generally, automated static analysis tools have difficulty detecting custom authorization schemes. In addition, the software's design may include some functionality that is accessible to any user and does not require an authorization check; an automated technique that detects the absence of authorization may report false positives.

Effectiveness: Limited

Automated Dynamic Analysis

Automated dynamic analysis may find many or all possible interfaces that do not require authorization, but manual analysis is required to determine if the lack of authorization violates business logic

Manual Analysis

This weakness can be detected using tools and techniques that require manual (human) analysis, such as penetration testing, threat modeling, and interactive tools that allow the tester to record and modify an active session.

Specifically, manual static analysis is useful for evaluating the correctness of custom authorization mechanisms.

Effectiveness: Moderate

These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules. However, manual efforts might not achieve desired code coverage within limited time constraints.

Demonstrative Examples

Example 1

The following program could be part of a bulletin board system that allows users to send private messages to each other. This program intends to authenticate the user before deciding whether a private message should be displayed. Assume that LookupMessageObject() ensures that the $id argument is numeric, constructs a filename based on that id, and reads the message details from that file. Also assume that the program stores all private messages for all users in the same directory.

(Bad Code)

Example Language: **Perl**

```
sub DisplayPrivateMessage {
my($id) = @_;
my $Message = LookupMessageObject($id);
print "From: " . encodeHTML($Message->{from}) . "<br>\n";
print "Subject: " . encodeHTML($Message->{subject}) . "\n";
print "<hr>\n";
print "Body: " . encodeHTML($Message->{body}) . "\n";
}

my $q = new CGI;
# For purposes of this example, assume that CWE-309 and
# CWE-523 do not apply.
if (! AuthenticateUser($q->param('username'), $q->param('password'))) {
ExitError("invalid username or password");
}

my $id = $q->param('id');
DisplayPrivateMessage($id);
```

While the program properly exits if authentication fails, it does not ensure that the message is addressed to the user. As a result, an authenticated attacker could provide any arbitrary identifier and read private messages that were intended for other users.

One way to avoid this problem would be to ensure that the "to" field in the message object matches the username of the authenticated user.

Observed Examples

Reference	Description
CVE-2009-3168	Web application does not restrict access to admin scripts, allowing authenticated users to reset administrative passwords.

CVE-2009-2960	Web application does not restrict access to admin scripts, allowing authenticated users to modify passwords of other users.
CVE-2009-3597	Web application stores database file under the web root with insufficient access control (CWE-219), allowing direct request.
CVE-2009-2282	Terminal server does not check authorization for guest access.
CVE-2009-3230	Database server does not use appropriate privileges for certain sensitive operations.
CVE-2009-2213	Gateway uses default "Allow" configuration for its authorization settings.
CVE-2009-0034	Chain: product does not properly interpret a configuration option for a system group, allowing users to gain privileges.
CVE-2008-6123	Chain: SNMP product does not properly parse a configuration option for which hosts are allowed to connect, allowing unauthorized IP addresses to connect.
CVE-2008-5027	System monitoring software allows users to bypass authorization by creating custom forms.
CVE-2008-7109	Chain: reliance on client-side security (CWE-602) allows attackers to bypass authorization using a custom client.
CVE-2008-3424	Chain: product does not properly handle wildcards in an authorization policy list, allowing unintended access.
CVE-2009-3781	Content management system does not check access permissions for private files, allowing others to view those files.
CVE-2008-4577	ACL-based protection mechanism treats negative access rights as if they are positive, allowing bypass of intended restrictions.
CVE-2008-6548	Product does not check the ACL of a page accessed using an "include" directive, allowing attackers to read unauthorized files.
CVE-2007-2925	Default ACL list for a DNS server does not set certain ACLs, allowing unauthorized DNS queries.
CVE-2006-6679	Product relies on the X-Forwarded-For HTTP header for authorization, allowing unintended access by spoofing the header.
CVE-2005-3623	OS kernel does not check for a certain privilege before setting ACLs for files.
CVE-2005-2801	Chain: file-system code performs an incorrect comparison (CWE-697), preventing defauls ACLs from being properly applied.
CVE-2001-1155	Chain: product does not properly check the result of a reverse DNS lookup because of operator precedence (CWE-783), allowing bypass of DNS-based access restrictions.

Potential Mitigations

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully mapping roles with data and functionality. Use role-based access control (RBAC) to enforce the roles at the appropriate boundaries.

Note that this approach may not protect against horizontal authorization, i.e., it will not protect a user from attacking others with the same role.

Phase: Architecture and Design

Ensure that you perform access control checks related to your business logic. These checks may be different than the access control checks that you apply to more generic resources such as files, connections, processes, memory, and database records. For example, a database may restrict access for medical records to a specific database user, but each record might only be intended to be accessible to the patient and the patient's doctor.

Phase: Architecture and Design

Strategy: Libraries or Frameworks

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness

easier to avoid.

For example, consider using authorization frameworks such as the JAAS Authorization Framework and the OWASP ESAPI Access Control feature.

Phase: Architecture and Design

For web applications, make sure that the access control mechanism is enforced correctly at the server side on every page. Users should not be able to access any unauthorized functionality or information by simply requesting direct access to that page.

One way to do this is to ensure that all pages containing sensitive information are not cached, and that all such pages restrict access to requests that are accompanied by an active and authenticated session token associated with a user who has the required permissions to access that page.

Phases: System Configuration; Installation

Use the access control capabilities of your operating system and server environment and define your access control lists accordingly. Use a "default deny" policy when defining these ACLs.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	254	Security Features	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Class	284	Access Control (Authorization) Issues	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	**Weaknesses in OWASP Top Ten (2007) (primary)629**
ChildOf	Category	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	**Weaknesses in OWASP Top Ten (2004) (primary)711**
ChildOf	Category	753	2009 Top 25 - Porous Defenses	**Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)750**
ChildOf	Category	803	2010 Top 25 - Porous Defenses	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
ParentOf	Weakness Variant	219	Sensitive Data Under Web Root	**Research Concepts (primary)1000**
ParentOf	Weakness Base	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Class	638	Failure to Use Complete Mediation	Research Concepts1000
ParentOf	Weakness Base	804	Guessable CAPTCHA	**Development Concepts (primary)699 Research Concepts (primary)1000**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
7 Pernicious Kingdoms			Missing Access Control
OWASP Top Ten 2007	A10	CWE More Specific	Failure to Restrict URL Access
OWASP Top Ten 2004	A2	CWE More Specific	Broken Access Control

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
1	Accessing Functionality Not Properly Constrained by ACLs	
13	Subverting Environment Variable Values	

17	Accessing, Modifying or Executing Executable Files
87	Forceful Browsing
39	Manipulating Opaque Client-based Data Tokens
45	Buffer Overflow via Symbolic Links
51	Poison Web Service Registry
59	Session Credential Falsification through Prediction
60	Reusing Session IDs (aka Session Replay)
77	Manipulating User-Controlled Variables
76	Manipulating Input to File System Calls
104	Cross Zone Scripting

References

NIST. "Role Based Access Control and Role Based Security". <http://csrc.nist.gov/groups/SNS/rbac/>.

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 4, "Authorization" Page 114; Chapter 6, "Determining Appropriate Access Control" Page 171. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	7 Pernicious Kingdoms		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-15		Veracode	External
	Suggested OWASP Top Ten 2004 mapping		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Other Notes, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Description, Likelihood of Exploit, Name, Other Notes, Potential Mitigations, References, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Description, Related Attack Patterns		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Relationships		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Type		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Relationships		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Detection Factors, Potential Mitigations, References, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-01-12	Missing or Inconsistent Access Control		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025