vul_files_24 Scan Report

Project Name	vul_files_24
Scan Start	Tuesday, January 7, 2025 10:24:25 AM
Preset	Checkmarx Default
Scan Time	02h:32m:04s
Lines Of Code Scanned	298848
Files Scanned	90
Report Creation Time	Tuesday, January 7, 2025 12:06:00 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (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

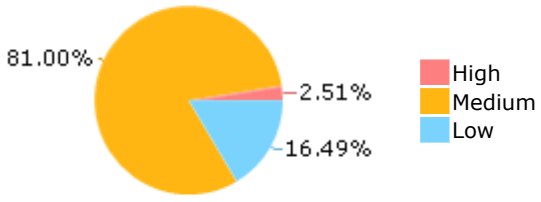
Results Limit

Results limit per query was set to 50

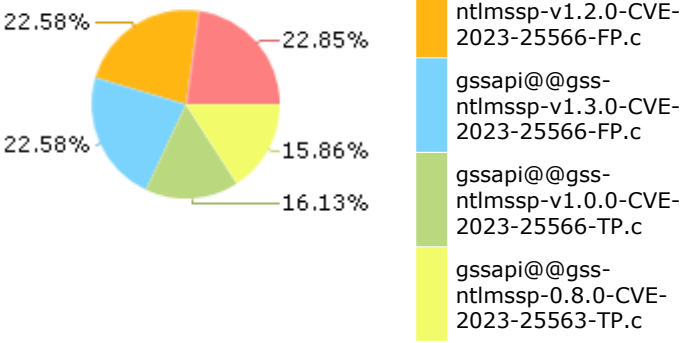
Selected Queries

Selected queries are listed in Result Summary

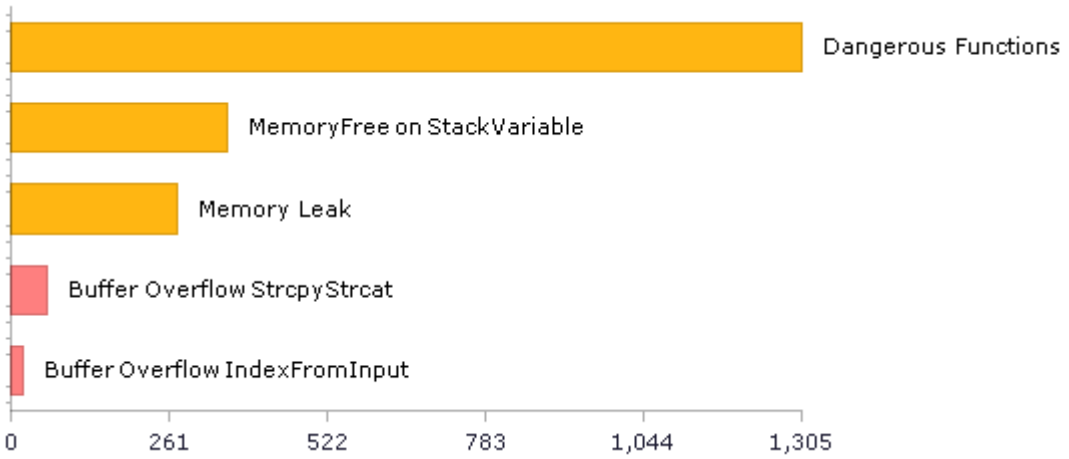
Result Summary



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	613	490
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	20	20
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control*	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS)	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities*	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	1305	1305
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	1305	1305
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	95	95
PCI DSS (3.2) - 6.5.2 - Buffer overflows	341	341
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.	6	6
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.	20	20
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	6	6

***** 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)	20	20
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	0	0
SC-28 Protection of Information at Rest (P1)	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)*	690	385
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	217	217
SI-11 Error Handling (P2)*	76	76
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	166	127

***** 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

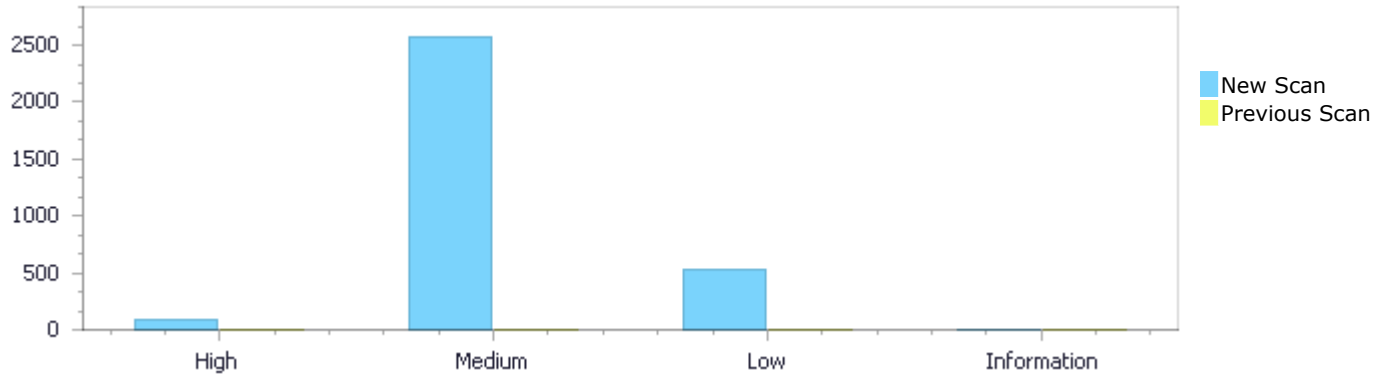
	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, 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	80	2,579	525	0	3,184
Recurrent Issues	0	0	0	0	0
Total	80	2,579	525	0	3,184
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	80	2,579	525	0	3,184
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	80	2,579	525	0	3,184

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow StrcpyStrcat	60	High
Buffer Overflow IndexFromInput	20	High
Dangerous Functions	1305	Medium
MemoryFree on StackVariable	358	Medium
Memory Leak	275	Medium

Buffer Overflow boundcpy WrongSizeParam	267	Medium
Use of Zero Initialized Pointer	246	Medium
Double Free	71	Medium
Wrong Size t Allocation	31	Medium
Use of Uninitialized Variable	12	Medium
Char Overflow	8	Medium
Integer Overflow	6	Medium
NULL Pointer Dereference	151	Low
Unchecked Array Index	123	Low
Potential Off by One Error in Loops	95	Low
Unchecked Return Value	76	Low
Improper Resource Access Authorization	20	Low
Potential Precision Problem	20	Low
TOCTOU	20	Low
Use of Sizeof On a Pointer Type	14	Low
Arithmenic Operation On Boolean	6	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	79
gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	78
gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	78
gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	56
gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	56
gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	56
gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	56
gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	56
gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c	56
gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c	56

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=1000032&projectid=26&pathid=1
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v555-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v555-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v555-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that homefile passes to filename, at line 250 of gwsw@@less-v555-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3
Status New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v555-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v555-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	301	374
Object	s	to

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method fexpand(s)

```
....
301.        char *s;
....
374.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=4
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v555-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v555-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=5
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v555-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v555-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=6
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v555-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v555-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	301	374
Object	s	to

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
301.        char *s;
....
374.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=7
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v564-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v564-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=8
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v564-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v564-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=9
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v564-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v564-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	301	374
Object	s	to

Code Snippet	
File Name	gwsw@@less-v564-CVE-2022-48624-TP.c
Method	fexpand(s)

```
....
301.        char *s;
....
374.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=10
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v564-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v564-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	136	198
Object	s	p

Code Snippet	
File Name	gwsw@@less-v564-CVE-2024-32487-TP.c
Method	shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=11
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v564-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v564-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-	gwsw@@less-v564-CVE-2024-32487-

	TP.c	TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=12
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v564-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v564-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	301	374
Object	s	to

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
301.        char *s;
....
374.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=13
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v568-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v568-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 14:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=14
Status New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v568-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v568-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=15
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v568-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v568-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	301	374
Object	s	to

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method fexpand(s)

```
....
301.        char *s;
....
374.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=16
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v568-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v568-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=17
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v568-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v568-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=18
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v568-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v568-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	301	374
Object	s	to

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
301.        char *s;
....
374.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=19
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v580-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v580-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v580-CVE-2022-48624-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=20
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v580-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v580-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	251	280
Object	filename	res

Code Snippet	
File Name	gwsw@@less-v580-CVE-2022-48624-TP.c
Method	homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=21
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v580-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 300 of gwsw@@less-v580-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	301	374
Object	s	to

Code Snippet	
File Name	gwsw@@less-v580-CVE-2022-48624-TP.c
Method	fexpand(s)

```
....
301.        char *s;
....
374.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=22
Status	New

The size of the buffer used by shell_quote in p, at line 135 of gwsw@@less-v580-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 135 of gwsw@@less-v580-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-	gwsw@@less-v580-CVE-2024-32487-

	TP.c	TP.c
Line	136	198
Object	s	p

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
136.        char *s;
....
198.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=23
Status	New

The size of the buffer used by homefile in res, at line 250 of gwsw@@less-v580-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 250 of gwsw@@less-v580-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	251	280
Object	filename	res

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
251.        char *filename;
....
280.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=24
Status	New

The size of the buffer used by fexpand in to, at line 300 of gwsw@@less-v580-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that fexpand passes to s, at line 300 of gwsw@@less-v580-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	301	374
Object	s	to

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
301.        char *s;
....
374.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 25:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=25
Status New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v590-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v590-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 26:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=26
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v590-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v590-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=27
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v590-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v590-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=28
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v590-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v590-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=29
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v590-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v590-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=30
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v590-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v590-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=31
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v594-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v594-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	143	205
Object	s	p

Code Snippet	
File Name	gwsw@@less-v594-CVE-2022-48624-TP.c
Method	shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 32:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=32
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v594-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v594-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	262	285
Object	filename	res

Code Snippet	
File Name	gwsw@@less-v594-CVE-2022-48624-TP.c
Method	homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=33
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v594-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v594-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-	gwsw@@less-v594-CVE-2022-48624-

	TP.c	TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v594-CVE-2022-48624-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=34
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v594-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v594-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=35
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v594-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that homefile passes to filename, at line 261 of gwsw@@less-v594-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 36:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=36
Status New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v594-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v594-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 37:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=37
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v600-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v600-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=38
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v600-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v600-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=39
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v600-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v600-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=40
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v600-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v600-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=41
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v600-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v600-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=42
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v600-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v600-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	306	379
Object	s	to

Code Snippet	
File Name	gwsw@@less-v600-CVE-2024-32487-TP.c
Method	fexpand(s)

```
....
306.        char *s;
....
379.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=43
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v605-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v605-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	143	205
Object	s	p

Code Snippet	
File Name	gwsw@@less-v605-CVE-2022-48624-TP.c
Method	shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=44
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v605-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v605-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-	gwsw@@less-v605-CVE-2022-48624-

	TP.c	TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=45
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v605-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v605-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=46
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v605-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the

source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v605-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 47:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=47
Status New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v605-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v605-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow StrcpyStrcat\Path 48:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=48
Status	New

The size of the buffer used by fexpand in to, at line 305 of gwsw@@less-v605-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that fexpand passes to s, at line 305 of gwsw@@less-v605-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	306	379
Object	s	to

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method fexpand(s)

```
....
306.        char *s;
....
379.                                    strcpy(to, get_filename(ifile));
```

Buffer Overflow StrcpyStrcat\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=49
Status	New

The size of the buffer used by shell_quote in p, at line 142 of gwsw@@less-v609-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that shell_quote passes to s, at line 142 of gwsw@@less-v609-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	143	205
Object	s	p

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method shell_quote(s)

```
....
143.        char *s;
....
205.                            strcpy(p, esc);
```

Buffer Overflow StrcpyStrcat\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=50
Status	New

The size of the buffer used by homefile in res, at line 261 of gwsw@@less-v609-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that homefile passes to filename, at line 261 of gwsw@@less-v609-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	262	285
Object	filename	res

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method homefile(filename)

```
....
262.        char *filename;
....
285.                    strcpy(pathname, res);
```

Buffer Overflow IndexFromInput

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

Categories

OWASP Top 10 2017: A1-Injection

Description

Buffer Overflow IndexFromInput\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=61
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v555-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v555-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	469	472

Object	data	n

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.         n = read(f, data, sizeof(data));
....
472.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=62
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v555-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v555-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
469.         n = read(f, data, sizeof(data));
....
472.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=63
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v564-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v564-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.         n = read(f, data, sizeof(data));
....
472.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=64
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v564-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v564-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
469.         n = read(f, data, sizeof(data));
....
472.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=65
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v568-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v568-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
....
472.        edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 6:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=66
Status New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v568-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v568-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
....
472.        edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 7:

Severity High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=67
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v580-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v580-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v580-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.         n = read(f, data, sizeof(data));
....
472.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=68
Status	New

The size of the buffer used by bin_file in n, at line 456 of gwsw@@less-v580-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 456 of gwsw@@less-v580-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	469	472
Object	data	n

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
....
472.        edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=69
Status	New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v590-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v590-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
....
477.        edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=70
Status	New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v590-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v590-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 11:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=71
Status New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v594-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v594-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v594-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 12:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=72
Status New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v594-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v594-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-	gwsw@@less-v594-CVE-2024-32487-

	TP.c	TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=73
Status	New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v600-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v600-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=74
Status	New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v600-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that bin_file passes to data, at line 461 of gwsw@@less-v600-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 15:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=75
Status New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v605-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v605-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 16:

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=76
Status	New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v605-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v605-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=77
Status	New

The size of the buffer used by bin_file in n, at line 461 of gwsw@@less-v609-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 461 of gwsw@@less-v609-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	474	477
Object	data	n

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.         n = read(f, data, sizeof(data));
....
477.         edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 18:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=78
Status	New

The size of the buffer used by bin_file in n, at line 446 of gwsw@@less-v624-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 446 of gwsw@@less-v624-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v624-CVE-2024-32487-TP.c	gwsw@@less-v624-CVE-2024-32487-TP.c
Line	458	461
Object	data	n

Code Snippet
File Name gwsw@@less-v624-CVE-2024-32487-TP.c
Method public int bin_file(int f)

```
....
458.        n = read(f, data, sizeof(data));
....
461.        edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=79
Status	New

The size of the buffer used by bin_file in n, at line 446 of gwsw@@less-v634-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 446 of gwsw@@less-v634-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v634-CVE-2024-32487-TP.c	gwsw@@less-v634-CVE-2024-32487-TP.c
Line	458	461
Object	data	n

Code Snippet
File Name gwsw@@less-v634-CVE-2024-32487-TP.c
Method public int bin_file(int f)

```
....
458.        n = read(f, data, sizeof(data));
....
461.        edata = &data[n];
```

Buffer Overflow IndexFromInput\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=80
Status	New

The size of the buffer used by bin_file in n, at line 446 of gwsw@@less-v644-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that bin_file passes to data, at line 446 of gwsw@@less-v644-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v644-CVE-2024-32487-TP.c	gwsw@@less-v644-CVE-2024-32487-TP.c
Line	458	461
Object	data	n

Code Snippet
File Name gwsw@@less-v644-CVE-2024-32487-TP.c
Method public int bin_file(int f)

```
....
458.        n = read(f, data, sizeof(data));
....
461.        edata = &data[n];
```

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=1000032&projectid=26&pathid=393
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1346	1346
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1346.          memcpy(mic->data, &buffer->data[payload_offs], 16);
```

Dangerous Functions\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=394
Status New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1377	1377
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1377.                  memcpy(target_info->data, data, len);
```

Dangerous Functions\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=395
Status New

The dangerous function, memcpy, was found in use at line 233 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static void ntlm_encode_header(struct wire_msg_hdr *hdr, uint32_t msg_type)

```
....
235.      memcpy(hdr->signature, ntlmssp_sig, 8);
```

Dangerous Functions\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=396
Status New

The dangerous function, memcpy, was found in use at line 249 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	258	258
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_oem_str(struct wire_field_hdr *hdr,

```
....
258.      memcpy(&buffer->data[*data_offs], str, str_len);
```

Dangerous Functions\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=397

Status	New

The dangerous function, memcpy, was found in use at line 372 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	380	380
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
380.      memcpy(&buffer->data[*data_offs], &ntlmssp_version,
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=398
Status	New

The dangerous function, memcpy, was found in use at line 386 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_field(struct wire_field_hdr *hdr,

```
....
395.      memcpy(&buffer->data[*data_offs], field->data, field->length);
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=399
Status	New

The dangerous function, memcpy, was found in use at line 404 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	427	427
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
427.      memcpy(b.data, &buffer->data[offs], b.length);
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=400
Status	New

The dangerous function, memcpy, was found in use at line 486 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	501	501
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_av_pair_value(struct ntlm_buffer *buffer,

```
....
501.          memcpy(av_pair->value, value->data, value->length);
```

Dangerous Functions\Path 9:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=401
Status	New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	708	708
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
708.                memcpy(&timestamp, av_pair->value, sizeof(timestamp));
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=402
Status	New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	713	713
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
713.                memcpy(&flags, av_pair->value, sizeof(flags));
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=403
Status	New

The dangerous function, memcpy, was found in use at line 1008 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1076	1076
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_chal_msg(struct ntlm_ctx *ctx,

```
....
1076.       memcpy(msg->server_challenge, challenge->data, 8);
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=404
Status	New

The dangerous function, memcpy, was found in use at line 1093 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1126	1126
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_chal_msg(struct ntlm_ctx *ctx,

```
....
1126.       memcpy(challenge->data, msg->server_challenge, 8);
```

Dangerous Functions\Path 13:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=405
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1346	1346
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1346.          memcpy(mic->data, &buffer->data[payload_offs], 16);
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=406
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1377	1377
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1377.                  memcpy(target_info->data, data, len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=407
Status	New

The dangerous function, memcpy, was found in use at line 233 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static void ntlm_encode_header(struct wire_msg_hdr *hdr, uint32_t msg_type)

```
....
235.      memcpy(hdr->signature, ntlmssp_sig, 8);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=408
Status	New

The dangerous function, memcpy, was found in use at line 249 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	258	258
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_encode_oem_str(struct wire_field_hdr *hdr,

```
....
258.      memcpy(&buffer->data[*data_offs], str, str_len);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=409
Status	New

The dangerous function, memcpy, was found in use at line 372 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	380	380
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
380.      memcpy(&buffer->data[*data_offs], &ntlmssp_version,
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=410
Status	New

The dangerous function, memcpy, was found in use at line 386 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_encode_field(struct wire_field_hdr *hdr,

```
....
395.      memcpy(&buffer->data[*data_offs], field->data, field->length);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=411
Status	New

The dangerous function, memcpy, was found in use at line 404 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	427	427
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
427.      memcpy(b.data, &buffer->data[offs], b.length);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=412
Status	New

The dangerous function, memcpy, was found in use at line 486 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	501	501
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_encode_av_pair_value(struct ntlm_buffer *buffer,

```
....
501.          memcpy(av_pair->value, value->data, value->length);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=413
Status	New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	708	708
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
708.              memcpy(&timestamp, av_pair->value, sizeof(timestamp));
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=414
Status	New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	713	713
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method	int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
713.              memcpy(&flags, av_pair->value, sizeof(flags));
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=415
Status	New

The dangerous function, memcpy, was found in use at line 1008 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1076	1076
Object	memcpy	memcpy

Code Snippet

File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method	int ntlm_encode_chal_msg(struct ntlm_ctx *ctx,

```
....
1076.      memcpy(msg->server_challenge, challenge->data, 8);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=416
Status	New

The dangerous function, memcpy, was found in use at line 1093 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1126	1126
Object	memcpy	memcpy

Code Snippet

File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method	int ntlm_decode_chal_msg(struct ntlm_ctx *ctx,

```
....
1126.       memcpy(challenge->data, msg->server_challenge, 8);
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=417
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	1346	1346
Object	memcpy	memcpy

Code Snippet

File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method	int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1346.           memcpy(mic->data, &buffer->data[payload_offs], 16);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=418
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	1377	1377
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1377.                   memcpy(target_info->data, data, len);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=419
Status	New

The dangerous function, memcpy, was found in use at line 233 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static void ntlm_encode_header(struct wire_msg_hdr *hdr, uint32_t msg_type)

```
....
235.      memcpy(hdr->signature, ntlmssp_sig, 8);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=420
Status	New

The dangerous function, memcpy, was found in use at line 249 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	258	258
Object	memcpy	memcpy

Code Snippet	
File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method	static int ntlm_encode_oem_str(struct wire_field_hdr *hdr,

```
....
258.      memcpy(&buffer->data[*data_offs], str, str_len);
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=421
Status	New

The dangerous function, memcpy, was found in use at line 372 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	380	380
Object	memcpy	memcpy

Code Snippet	
File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method	static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
380.      memcpy(&buffer->data[*data_offs], &ntlmssp_version,
```

Dangerous Functions\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=422
Status	New

The dangerous function, memcpy, was found in use at line 386 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	395	395

Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_encode_field(struct wire_field_hdr *hdr,

```
....
395.      memcpy(&buffer->data[*data_offs], field->data, field->length);
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=423
Status	New

The dangerous function, memcpy, was found in use at line 404 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	427	427
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
427.      memcpy(b.data, &buffer->data[offs], b.length);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=424
Status	New

The dangerous function, memcpy, was found in use at line 486 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Line	501	501
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_encode_av_pair_value(struct ntlm_buffer *buffer,

```
....
501.          memcpy(av_pair->value, value->data, value->length);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=425
Status	New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	708	708
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
708.              memcpy(&timestamp, av_pair->value, sizeof(timestamp));
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=426
Status	New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-

	25565-TP.c	25565-TP.c
Line	713	713
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
713.              memcpy(&flags, av_pair->value, sizeof(flags));
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=427
Status	New

The dangerous function, memcpy, was found in use at line 1008 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	1076	1076
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_chal_msg(struct ntlm_ctx *ctx,

```
....
1076.      memcpy(msg->server_challenge, challenge->data, 8);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=428
Status	New

The dangerous function, memcpy, was found in use at line 1093 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	1126	1126
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_chal_msg(struct ntlm_ctx *ctx,

```
....
1126.      memcpy(challenge->data, msg->server_challenge, 8);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=429
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	1346	1346
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1346.          memcpy(mic->data, &buffer->data[payload_offs], 16);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=430
Status	New

The dangerous function, memcpy, was found in use at line 1305 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	1377	1377
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1377.                   memcpy(target_info->data, data, len);
```

Dangerous Functions\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=431
Status New

The dangerous function, memcpy, was found in use at line 233 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	235	235
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static void ntlm_encode_header(struct wire_msg_hdr *hdr, uint32_t msg_type)

```
....
235.      memcpy(hdr->signature, ntlmssp_sig, 8);
```

Dangerous Functions\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=432
Status New

The dangerous function, memcpy, was found in use at line 249 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	258	258
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_oem_str(struct wire_field_hdr *hdr,

```
....
258.      memcpy(&buffer->data[*data_offs], str, str_len);
```

Dangerous Functions\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=433
Status New

The dangerous function, memcpy, was found in use at line 372 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	380	380
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
380.      memcpy(&buffer->data[*data_offs], &ntlmssp_version,
```

Dangerous Functions\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=434
Status New

The dangerous function, memcpy, was found in use at line 386 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	395	395
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_field(struct wire_field_hdr *hdr,

```
....
395.      memcpy(&buffer->data[*data_offs], field->data, field->length);
```

Dangerous Functions\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=435
Status New

The dangerous function, memcpy, was found in use at line 404 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	427	427
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
427.      memcpy(b.data, &buffer->data[offs], b.length);
```

Dangerous Functions\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=436
Status New

The dangerous function, memcpy, was found in use at line 486 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	501	501
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_av_pair_value(struct ntlm_buffer *buffer,

```
....
501.          memcpy(av_pair->value, value->data, value->length);
```

Dangerous Functions\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=437
Status New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	708	708
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
708.              memcpy(&timestamp, av_pair->value, sizeof(timestamp));
```

Dangerous Functions\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=438
Status New

The dangerous function, memcpy, was found in use at line 655 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	713	713
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
713.              memcpy(&flags, av_pair->value, sizeof(flags));
```

Dangerous Functions\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=439
Status New

The dangerous function, memcpy, was found in use at line 1008 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	1076	1076
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_encode_chal_msg(struct ntlm_ctx *ctx,

```
....
1076.      memcpy(msg->server_challenge, challenge->data, 8);
```

Dangerous Functions\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=440
Status New

The dangerous function, memcpy, was found in use at line 1093 in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	1126	1126
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_chal_msg(struct ntlm_ctx *ctx,

```
....
1126.       memcpy(challenge->data, msg->server_challenge, 8);
```

Dangerous Functions\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=441
Status New

The dangerous function, memcpy, was found in use at line 1284 in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	1325	1325
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1325.           memcpy(mic->data, &buffer->data[payload_offs], 16);
```

Dangerous Functions\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=442
Status New

The dangerous function, memcpy, was found in use at line 1284 in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	1356	1356
Object	memcpy	memcpy

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1356.                   memcpy(target_info->data, data, len);
```

MemoryFree on StackVariable

Query Path:
CPP\Cx\CPP Medium Threat\MemoryFree on StackVariable Version:0

Description

MemoryFree on StackVariable\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1769
Status	New

Calling free() (line 20) on a variable that was not dynamically allocated (line 20) in file gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	59	59
Object	r1	r1

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
59.           free(r1);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1770
Status	New

Calling free() (line 20) on a variable that was not dynamically allocated (line 20) in file gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	60	60
Object	r2	r2

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
60.             free(r2);
```

MemoryFree on StackVariable\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1771
Status New

Calling free() (line 25) on a variable that was not dynamically allocated (line 25) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	64	64
Object	r1	r1

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
64.             free(r1);
```

MemoryFree on StackVariable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1772
Status New

Calling free() (line 25) on a variable that was not dynamically allocated (line 25) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	65	65
Object	r2	r2

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
65.             free(r2);
```

MemoryFree on StackVariable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1773
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	304	304
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
304.                    free(spn);
```

MemoryFree on StackVariable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1774
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	319	319
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
319.                    free(spn);
```

MemoryFree on StackVariable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1775
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	330	330
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.                    free(spn);
```

MemoryFree on StackVariable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1776
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	340	340
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
340.                        free(spn);
```

MemoryFree on StackVariable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1777
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	346	346
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
346.                        free(spn);
```

MemoryFree on StackVariable\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1778
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	353	353
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
353.                    free(spn);
```

MemoryFree on StackVariable\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1779
Status New

Calling free() (line 263) on a variable that was not dynamically allocated (line 263) in file gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	358	358
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
358.            free(spn);
```

MemoryFree on StackVariable\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1780
Status New

Calling free() (line 25) on a variable that was not dynamically allocated (line 25) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	64	64
Object	r1	r1

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
64.             free(r1);
```

MemoryFree on StackVariable\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1781
Status New

Calling free() (line 25) on a variable that was not dynamically allocated (line 25) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	65	65
Object	r2	r2

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
65.             free(r2);
```

MemoryFree on StackVariable\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1782
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	300	300
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
300.                    free(spn);
```

MemoryFree on StackVariable\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1783
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	315	315
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
315.                    free(spn);
```

MemoryFree on StackVariable\Path 16:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1784
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	326	326
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
```

MemoryFree on StackVariable\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1785
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	336	336
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                    free(spn);
```

MemoryFree on StackVariable\Path 18:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1786
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	342	342
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
342.                        free(spn);
```

MemoryFree on StackVariable\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1787
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	349	349
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
349.                    free(spn);
```

MemoryFree on StackVariable\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1788
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	354	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
354.            free(spn);
```

MemoryFree on StackVariable\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1789
Status New

Calling free() (line 25) on a variable that was not dynamically allocated (line 25) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	64	64
Object	r1	r1

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
64.             free(r1);
```

MemoryFree on StackVariable\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1790
Status New

Calling free() (line 25) on a variable that was not dynamically allocated (line 25) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	65	65
Object	r2	r2

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method static uint32_t string_split(uint32_t *minor_status, char sep,

```
....
65.           free(r2);
```

MemoryFree on StackVariable\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1791
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	300	300
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
300.                    free(spn);
```

MemoryFree on StackVariable\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1792
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	315	315
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
315.                    free(spn);
```

MemoryFree on StackVariable\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1793
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	326	326
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
```

MemoryFree on StackVariable\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1794
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	336	336
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
```

MemoryFree on StackVariable\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1795
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	342	342
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
342.                        free(spn);
```

MemoryFree on StackVariable\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1796
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	349	349
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
349.                    free(spn);
```

MemoryFree on StackVariable\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1797
Status New

Calling free() (line 259) on a variable that was not dynamically allocated (line 259) in file gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c may result with a crash.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	354	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
354.            free(spn);
```

MemoryFree on StackVariable\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1798
Status New

Calling free() (line 396) on a variable that was not dynamically allocated (line 396) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	442	442
Object	qs	qs

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
442.                free(qs);
```

MemoryFree on StackVariable\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1799
Status New

Calling free() (line 396) on a variable that was not dynamically allocated (line 396) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	446	446
Object	fpat	fpat

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
446.        free(fpat);
```

MemoryFree on StackVariable\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1800
Status New

Calling free() (line 515) on a variable that was not dynamically allocated (line 515) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	543	543
Object	buf	buf

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method readfd(fd)

```
....
543.                    free(buf);
```

MemoryFree on StackVariable\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1801
Status New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	589	589
Object	esccmd	esccmd

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method shellcmd(cmd)

```
....
589.                    free(esccmd);
```

MemoryFree on StackVariable\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1802
Status New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	591	591
Object	scmd	scmd

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method shellcmd(cmd)

```
....
591.                    free(scmd);
```

MemoryFree on StackVariable\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1803
Status New

Calling free() (line 613) on a variable that was not dynamically allocated (line 613) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	645	645
Object	qfilename	qfilename

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
645.                    free(qfilename);
```

MemoryFree on StackVariable\Path 36:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1804
Status New

Calling free() (line 613) on a variable that was not dynamically allocated (line 613) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	656	656
Object	qfilename	qfilename

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
656.                    free(qfilename);
```

MemoryFree on StackVariable\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1805
Status New

Calling free() (line 954) on a variable that was not dynamically allocated (line 954) in file gwsw@@less-v555-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	978	978
Object	cmd	cmd

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method close_altfile(altfilename, filename)

```
....
978.        free(cmd);
```

MemoryFree on StackVariable\Path 38:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1806
Status New

Calling free() (line 396) on a variable that was not dynamically allocated (line 396) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	442	442
Object	qs	qs

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method fcomplete(s)

```
....
442.                free(qs);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1807
Status	New

Calling free() (line 396) on a variable that was not dynamically allocated (line 396) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	446	446
Object	fpat	fpat

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method fcomplete(s)

```
....
446.          free(fpat);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1808
Status	New

Calling free() (line 515) on a variable that was not dynamically allocated (line 515) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	543	543
Object	buf	buf

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method readfd(fd)

```
....
543.                    free(buf);
```

MemoryFree on StackVariable\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1809
Status New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	589	589
Object	esccmd	esccmd

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method shellcmd(cmd)

```
....
589.                    free(esccmd);
```

MemoryFree on StackVariable\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1810
Status New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	591	591
Object	scmd	scmd

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method shellcmd(cmd)

```
....
591.                    free(scmd);
```

MemoryFree on StackVariable\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1811
Status New

Calling free() (line 613) on a variable that was not dynamically allocated (line 613) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	645	645
Object	qfilename	qfilename

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
645.                    free(qfilename);
```

MemoryFree on StackVariable\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1812
Status New

Calling free() (line 613) on a variable that was not dynamically allocated (line 613) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	656	656
Object	qfilename	qfilename

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
656.                    free(qfilename);
```

MemoryFree on StackVariable\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1813
Status New

Calling free() (line 954) on a variable that was not dynamically allocated (line 954) in file gwsw@@less-v555-CVE-2024-32487-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	978	978
Object	cmd	cmd

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method close_altfile(altfilename, filename)

```
....
978.        free(cmd);
```

MemoryFree on StackVariable\Path 46:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1814
Status New

Calling free() (line 396) on a variable that was not dynamically allocated (line 396) in file gwsw@@less-v564-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	442	442
Object	qs	qs

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
442.                free(qs);
```

MemoryFree on StackVariable\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1815
Status New

Calling free() (line 396) on a variable that was not dynamically allocated (line 396) in file gwsw@@less-v564-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	446	446
Object	fpat	fpat

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
446.          free(fpat);
```

MemoryFree on StackVariable\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1816
Status New

Calling free() (line 515) on a variable that was not dynamically allocated (line 515) in file gwsw@@less-v564-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	543	543
Object	buf	buf

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method readfd(fd)

```
....
543.                    free(buf);
```

MemoryFree on StackVariable\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1817
Status New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file gwsw@@less-v564-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	589	589
Object	esccmd	esccmd

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method shellcmd(cmd)

```
....
589.                    free(esccmd);
```

MemoryFree on StackVariable\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1818
Status New

Calling free() (line 562) on a variable that was not dynamically allocated (line 562) in file gwsw@@less-v564-CVE-2022-48624-TP.c may result with a crash.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	591	591
Object	scmd	scmd

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method shellcmd(cmd)

```
....
591.                    free(scmd);
```

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=1000032&projectid=26&pathid=2127
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	675	675
Object	uname	uname

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
675.          ret = asprintf(&uname, "%s\\%s",
```

Memory Leak\Path 2:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2128
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	734	734
Object	uname	uname

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
734.          ret = asprintf(&uname, "%s\\%s",
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2129
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	730	730
Object	uname	uname

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
730.          ret = asprintf(&uname, "%s\\%s",
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2130
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-

	25566-FP.c	25566-FP.c
Line	730	730
Object	uname	uname

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
730.          ret = asprintf(&uname, "%s\\%s",
```

Memory Leak\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2131
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	615	615
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_display_name(uint32_t *minor_status,

```
....
615.              ret = asprintf((char **)&out->value, "%s\\%s",
```

Memory Leak\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2132
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	674	674
Object	out	out

Code Snippet

File Name	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method	uint32_t gssntlm_display_name(uint32_t *minor_status,

```
....
674.              ret = asprintf((char **)&out->value, "%s\\%s",
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2133
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	670	670
Object	out	out

Code Snippet

File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_display_name(uint32_t *minor_status,

```
....
670.              ret = asprintf((char **)&out->value, "%s\\%s",
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2134
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	670	670
Object	out	out

Code Snippet

File Name	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_display_name(uint32_t *minor_status,

```
....
670.              ret = asprintf((char **)&out->value, "%s\\%s",
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2135
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	124	124
Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
124.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2136
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1016	1016
Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1016.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2137
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	121	121
Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
121.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2138
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1037	1037
Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1037.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 13:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2139
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	121	121

Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
121.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 14:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2140
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	1201	1201
Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1201.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 15:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2141
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Line	123	123
Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
123.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2142
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Line	1206	1206
Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1206.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2143
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2022-38890-FP.c
Line	121	121
Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
121.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 18:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2144
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2022-38890-FP.c
Line	1218	1218
Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1218.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2145
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2022-38890-FP.c
Line	117	117
Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
117.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2146
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2022-38890-FP.c
Line	1162	1162
Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1162.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 21:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2147
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.8.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.8.0-CVE-2022-38890-FP.c
Line	118	118
Object	item	item

Code Snippet
File Name HandBrake@@HandBrake-1.8.0-CVE-2022-38890-FP.c
Method static void hb_qsv_add_new_dts(hb_list_t *list, int64_t new_dts)

```
....
118.          int64_t *item = malloc(sizeof(int64_t));
```

Memory Leak\Path 22:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2148
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.8.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.8.0-CVE-2022-38890-FP.c
Line	1161	1161

Object	pv	pv

Code Snippet
File Name HandBrake@@HandBrake-1.8.0-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1161.      hb_work_private_t *pv = calloc(1, sizeof(hb_work_private_t));
```

Memory Leak\Path 23:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2149
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1372	1372
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1372.                  target_info->data = malloc(len);
```

Memory Leak\Path 24:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2150
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	100	100
Object	_ctx	_ctx

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_init_ctx(struct ntlm_ctx **ctx)

```
....
100.      _ctx = calloc(1, sizeof(struct ntlm_ctx));
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2151
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	339	339
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
339.      out = malloc(str_len * 2 + 1);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2152
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	423	423
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
423.      b.data = malloc(len);
```

Memory Leak\Path 27:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2153
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2154
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	569	569
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2155
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	832	832
Object	av_target_name	av_target_name

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
832.          av_target_name = strdup(server);
```

Memory Leak\Path 30:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2156
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	933	933
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_neg_msg(struct ntlm_ctx *ctx, uint32_t flags,

```
....
933.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2157
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1049	1049

Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_chal_msg(struct ntlm_ctx *ctx,

```
....
1049.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 32:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2158
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	1221	1221
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_auth_msg(struct ntlm_ctx *ctx,

```
....
1221.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 33:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2159
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1372	1372
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1372.                   target_info->data = malloc(len);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2160
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	100	100
Object	_ctx	_ctx

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_init_ctx(struct ntlm_ctx **ctx)

```
....
100.      _ctx = calloc(1, sizeof(struct ntlm_ctx));
```

Memory Leak\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2161
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	339	339
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
339.      out = malloc(str_len * 2 + 1);
```

Memory Leak\Path 36:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2162
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	423	423
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
423.      b.data = malloc(len);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2163
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2164
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	569	569
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 39:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2165
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	832	832
Object	av_target_name	av_target_name

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
832.          av_target_name = strdup(server);
```

Memory Leak\Path 40:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2166
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	933	933

Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_neg_msg(struct ntlm_ctx *ctx, uint32_t flags,

```
....
933.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 41:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2167
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1049	1049
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_chal_msg(struct ntlm_ctx *ctx,

```
....
1049.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2168
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	1221	1221
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_auth_msg(struct ntlm_ctx *ctx,

```
....
1221.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2169
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	1372	1372
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_auth_msg(struct ntlm_ctx *ctx,

```
....
1372.                  target_info->data = malloc(len);
```

Memory Leak\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2170
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	100	100
Object	_ctx	_ctx

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_init_ctx(struct ntlm_ctx **ctx)

```
....
100.      _ctx = calloc(1, sizeof(struct ntlm_ctx));
```

Memory Leak\Path 45:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2171
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	339	339
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
339.      out = malloc(str_len * 2 + 1);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2172
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	423	423
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_field(struct wire_field_hdr *hdr,

```
....
423.      b.data = malloc(len);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2173
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Memory Leak\Path 48:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2174
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	569	569
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Memory Leak\Path 49:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2175
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	832	832

Object	av_target_name	av_target_name

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
832.          av_target_name = strdup(server);
```

Memory Leak\Path 50:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2176
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	933	933
Object	data	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_neg_msg(struct ntlm_ctx *ctx, uint32_t flags,

```
....
933.      buffer.data = calloc(1, buffer.length);
```

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=1000032&projectid=26&pathid=81
Status New

The size of the buffer used by ntlm_encode_version in wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer

overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	381	381
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
381.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=82
Status New

The size of the buffer used by ntlm_encode_version in wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	381	381
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
381.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=83
Status New

The size of the buffer used by ntlm_encode_version in wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	381	381
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
381.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=84
Status New

The size of the buffer used by ntlm_encode_version in wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 372 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	381	381
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
381.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=85
Status New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=86
Status New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=87

Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.            sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=88
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.            sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=89
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=90
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=91
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.            sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=92
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 350 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Line	359	359
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
359.            sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=93
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 352 of gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 352 of gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Line	361	361
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
361.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=94
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 352 of gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 352 of gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Line	361	361
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
361.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=95
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 354 of gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 354 of gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Line	363	363
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
363.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=96
Status	New

The size of the buffer used by ntlm_encode_version in wire_version, at line 354 of gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ntlm_encode_version passes to wire_version, at line 354 of gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c, to overwrite the target buffer.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Line	363	363
Object	wire_version	wire_version

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Method static int ntlm_encode_version(struct ntlm_ctx *ctx,

```
....
363.             sizeof(struct wire_version));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=97
Status	New

The size of the buffer used by hb_preset_apply_title in Namespace406120971, at line 1850 of HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_title passes to Namespace406120971, at line 1850 of HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	1884	1884
Object	Namespace406120971	Namespace406120971

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method int hb_preset_apply_title(hb_handle_t *h, int title_index,

```
....
1884.          memcpy(geo.crop, title->crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=98
Status	New

The size of the buffer used by hb_preset_apply_title in Namespace995404502, at line 1849 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_title passes to Namespace995404502, at line 1849 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	1883	1883
Object	Namespace995404502	Namespace995404502

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method int hb_preset_apply_title(hb_handle_t *h, int title_index,

```
....
1883.          memcpy(geo.crop, title->crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=99
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1485359770, at line 1958 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1485359770, at line 1958 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	2006	2006
Object	Namespace1485359770	Namespace1485359770

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2006.      memcpy(srcGeo.crop, title->crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=100
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1485359770, at line 1958 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1485359770, at line 1958 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	2024	2024
Object	Namespace1485359770	Namespace1485359770

Code Snippet	
File Name	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method	int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2024.          memcpy(geo.crop, srcGeo.crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=101
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1575471047, at line 1958 of HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1575471047, at line 1958 of HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	2006	2006
Object	Namespace1575471047	Namespace1575471047

Code Snippet	
File Name	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method	int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2006.      memcpy(srcGeo.crop, title->crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=102
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1575471047, at line 1958 of HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1575471047, at line 1958 of HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c

Line	2024	2024
Object	Namespace1575471047	Namespace1575471047

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2024.          memcpy(geo.crop, srcGeo.crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=103
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1704731228, at line 1968 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1704731228, at line 1968 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	2016	2016
Object	Namespace1704731228	Namespace1704731228

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2016.      memcpy(srcGeo.crop, title->crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=104
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1704731228, at line 1968 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1704731228, at line 1968 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	2028	2028
Object	Namespace1704731228	Namespace1704731228

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2028.            memcpy(geo.crop, srcGeo.crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=105
Status New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1704731228, at line 1968 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1704731228, at line 1968 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	2031	2031
Object	Namespace1704731228	Namespace1704731228

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2031.            memcpy(geo.crop, title->loose_crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=106
Status New

The size of the buffer used by hb_preset_apply_dimensions in Namespace851086843, at line 1974 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the

buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace851086843, at line 1974 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	2022	2022
Object	Namespace851086843	Namespace851086843

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2022.       memcpy(srcGeo.crop, title->crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=107
Status New

The size of the buffer used by hb_preset_apply_dimensions in Namespace851086843, at line 1974 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace851086843, at line 1974 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	2035	2035
Object	Namespace851086843	Namespace851086843

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2035.            memcpy(geo.crop, srcGeo.crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=108
Status New

The size of the buffer used by hb_preset_apply_dimensions in Namespace851086843, at line 1974 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace851086843, at line 1974 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	2038	2038
Object	Namespace851086843	Namespace851086843

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2038.            memcpy(geo.crop, title->loose_crop, sizeof(geo.crop));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=109
Status New

The size of the buffer used by gst_h265_parser_identify_and_split_nalu_hevc in GstH265NalUnit, at line 1606 of GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gst_h265_parser_identify_and_split_nalu_hevc passes to GstH265NalUnit, at line 1606 of GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c, to overwrite the target buffer.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	1694	1694
Object	GstH265NalUnit	GstH265NalUnit

Code Snippet
File Name GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method gst_h265_parser_identify_and_split_nalu_hevc (GstH265Parser * parser,

```
....
1694.      memset (&nalu, 0, sizeof (GstH265NalUnit));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=110
Status	New

The size of the buffer used by gst_h265_parser_identify_and_split_nalu_hevc in GstH265NalUnit, at line 1606 of GStreamer@@gstreamer-1.21.90-CVE-2023-40476-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gst_h265_parser_identify_and_split_nalu_hevc passes to GstH265NalUnit, at line 1606 of GStreamer@@gstreamer-1.21.90-CVE-2023-40476-TP.c, to overwrite the target buffer.

	Source	Destination
File	GStreamer@@gstreamer-1.21.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.90-CVE-2023-40476-TP.c
Line	1694	1694
Object	GstH265NalUnit	GstH265NalUnit

Code Snippet
File Name GStreamer@@gstreamer-1.21.90-CVE-2023-40476-TP.c
Method gst_h265_parser_identify_and_split_nalu_hevc (GstH265Parser * parser,

```
....
1694.       memset (&nalu, 0, sizeof (GstH265NalUnit));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=111
Status	New

The size of the buffer used by gst_h265_parser_identify_and_split_nalu_hevc in GstH265NalUnit, at line 1606 of GStreamer@@gstreamer-1.22.3-CVE-2023-40476-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that gst_h265_parser_identify_and_split_nalu_hevc passes to GstH265NalUnit, at line 1606 of GStreamer@@gstreamer-1.22.3-CVE-2023-40476-TP.c, to overwrite the target buffer.

	Source	Destination
File	GStreamer@@gstreamer-1.22.3-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.22.3-CVE-2023-40476-TP.c
Line	1694	1694
Object	GstH265NalUnit	GstH265NalUnit

Code Snippet
File Name GStreamer@@gstreamer-1.22.3-CVE-2023-40476-TP.c
Method gst_h265_parser_identify_and_split_nalu_hevc (GstH265Parser * parser,

```
....
1694.       memset (&nalu, 0, sizeof (GstH265NalUnit));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=112
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxBitstream, at line 292 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxBitstream, at line 292 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	304	304
Object	mfxBitstream	mfxBitstream

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
304.      memset(&bitstream,     0, sizeof(mfxBitstream));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=113
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxSyncPoint, at line 292 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxSyncPoint, at line 292 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	305	305
Object	mfxSyncPoint	mfxSyncPoint

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
305.      memset(&syncPoint,     0, sizeof(mfxSyncPoint));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=114
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxFrameSurface1, at line 292 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxFrameSurface1, at line 292 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	306	306
Object	mfxFrameSurface1	mfxFrameSurface1

Code Snippet

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
306.      memset(&frameSurface1, 0, sizeof(mfxFrameSurface1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=115
Status	New

The size of the buffer used by encqsvInit in mfxVideoParam, at line 1014 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that encqsvInit passes to mfxVideoParam, at line 1014 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1461	1461
Object	mfxVideoParam	mfxVideoParam

Code Snippet

File Name	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method	int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1461.      memset(&videoParam, 0, sizeof(mfxVideoParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=116
Status	New

The size of the buffer used by compute_init_delay in mfxVideoParam, at line 1851 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that compute_init_delay passes to mfxVideoParam, at line 1851 of HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1902	1902
Object	mfxVideoParam	mfxVideoParam

Code Snippet

File Name	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method	static void compute_init_delay(hb_work_private_t *pv, mfxBitstream *bs)

```
....
1902.                  memset(&videoParam, 0, sizeof(mfxVideoParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=117
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxBitstream, at line 289 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxBitstream, at line 289 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	301	301

Object	mfxBitstream	mfxBitstream

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
301.      memset(&bitstream,     0, sizeof(mfxBitstream));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=118
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxSyncPoint, at line 289 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxSyncPoint, at line 289 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	302	302
Object	mfxSyncPoint	mfxSyncPoint

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
302.      memset(&syncPoint,     0, sizeof(mfxSyncPoint));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=119
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxFrameSurface1, at line 289 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxFrameSurface1, at line 289 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination

File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	303	303
Object	mfxFrameSurface1	mfxFrameSurface1

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
303.      memset(&frameSurface1, 0, sizeof(mfxFrameSurface1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=120
Status	New

The size of the buffer used by encqsvInit in mfxVideoParam, at line 1035 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that encqsvInit passes to mfxVideoParam, at line 1035 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1496	1496
Object	mfxVideoParam	mfxVideoParam

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1496.      memset(&videoParam, 0, sizeof(mfxVideoParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=121
Status	New

The size of the buffer used by compute_init_delay in mfxVideoParam, at line 1878 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that compute_init_delay passes to

mfxVideoParam, at line 1878 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1929	1929
Object	mfxVideoParam	mfxVideoParam

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method static void compute_init_delay(hb_work_private_t *pv, mfxBitstream *bs)

```
....
1929.                   memset(&videoParam, 0, sizeof(mfxVideoParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=122
Status New

The size of the buffer used by qsv_hevc_make_header in mfxBitstream, at line 289 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxBitstream, at line 289 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	301	301
Object	mfxBitstream	mfxBitstream

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
301.      memset(&bitstream,     0, sizeof(mfxBitstream));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=123
Status New

The size of the buffer used by qsv_hevc_make_header in mfxSyncPoint, at line 289 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxSyncPoint, at line 289 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	302	302
Object	mfxSyncPoint	mfxSyncPoint

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
302.      memset(&syncPoint,     0, sizeof(mfxSyncPoint));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=124
Status New

The size of the buffer used by qsv_hevc_make_header in mfxFrameSurface1, at line 289 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxFrameSurface1, at line 289 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	303	303
Object	mfxFrameSurface1	mfxFrameSurface1

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
303.      memset(&frameSurface1, 0, sizeof(mfxFrameSurface1));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=125
Status	New

The size of the buffer used by encqsvInit in mfxVideoParam, at line 1199 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that encqsvInit passes to mfxVideoParam, at line 1199 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	1661	1661
Object	mfxVideoParam	mfxVideoParam

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1661.       memset(&videoParam, 0, sizeof(mfxVideoParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=126
Status	New

The size of the buffer used by compute_init_delay in mfxVideoParam, at line 1877 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that compute_init_delay passes to mfxVideoParam, at line 1877 of HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Line	1928	1928
Object	mfxVideoParam	mfxVideoParam

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2022-38890-FP.c
Method static void compute_init_delay(hb_work_private_t *pv, mfxBitstream *bs)

```
....
1928.                   memset(&videoParam, 0, sizeof(mfxVideoParam));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=127
Status	New

The size of the buffer used by hb_preset_apply_dimensions in Namespace1485359770, at line 1958 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hb_preset_apply_dimensions passes to Namespace1485359770, at line 1958 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	2038	2038
Object	Namespace1485359770	Namespace1485359770

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method int hb_preset_apply_dimensions(hb_handle_t *h, int title_index,

```
....
2038.           memset(geo.pad, 0, sizeof(geo.pad));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=128
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxBitstream, at line 291 of HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxBitstream, at line 291 of HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Line	303	303
Object	mfxBitstream	mfxBitstream

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
303.       memset(&bitstream,      0, sizeof(mfxBitstream));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=129
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxSyncPoint, at line 291 of HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxSyncPoint, at line 291 of HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Line	304	304
Object	mfxSyncPoint	mfxSyncPoint

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
304.      memset(&syncPoint,      0, sizeof(mfxSyncPoint));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=130
Status	New

The size of the buffer used by qsv_hevc_make_header in mfxFrameSurface1, at line 291 of HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qsv_hevc_make_header passes to mfxFrameSurface1, at line 291 of HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c, to overwrite the target buffer.

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Line	305	305
Object	mfxFrameSurface1	mfxFrameSurface1

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2022-38890-FP.c
Method static int qsv_hevc_make_header(hb_work_object_t *w, mfxSession session)

```
....
305.      memset(&frameSurface1, 0, sizeof(mfxFrameSurface1));
```

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=1000032&projectid=26&pathid=2776
Status	New

The variable declared in av_target_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	790	569
Object	av_target_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
790.      char *av_target_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2777
Status	New

The variable declared in dns_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	787	569
Object	dns_computer_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
787.      char *dns_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2778
Status	New

The variable declared in dns_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	788	569
Object	dns_domain_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
788.      char *dns_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2779
Status	New

The variable declared in dns_tree_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	789	569
Object	dns_tree_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
789.      char *dns_tree_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2780
Status	New

The variable declared in nb_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	785	569
Object	nb_computer_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
785.      char *nb_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2781
Status	New

The variable declared in nb_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	786	569
Object	nb_domain_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
786.      char *nb_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2782
Status	New

The variable declared in av_target at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	673	569
Object	av_target	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
673.      char *av_target = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2783
Status	New

The variable declared in dns_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Line	670	569
Object	dns_computer	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
670.      char *dns_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2784
Status	New

The variable declared in dns_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	671	569
Object	dns_domain	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
671.      char *dns_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2785
Status	New

The variable declared in dns_tree at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	672	569
Object	dns_tree	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
672.      char *dns_tree = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2786
Status	New

The variable declared in nb_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	668	569
Object	nb_computer	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
668.      char *nb_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2787
Status	New

The variable declared in nb_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	669	569
Object	nb_domain	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
669.      char *nb_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 13:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2788
Status	New

The variable declared in av_target_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	790	569
Object	av_target_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
790.      char *av_target_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2789
Status	New

The variable declared in dns_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	787	569
Object	dns_computer_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
787.      char *dns_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2790
Status	New

The variable declared in dns_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	788	569
Object	dns_domain_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
788.      char *dns_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2791
Status	New

The variable declared in dns_tree_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	789	569
Object	dns_tree_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
789.      char *dns_tree_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 17:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2792
Status New

The variable declared in nb_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	785	569
Object	nb_computer_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
785.      char *nb_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2793
Status	New

The variable declared in nb_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	786	569
Object	nb_domain_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
786.      char *nb_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2794
Status	New

The variable declared in av_target at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	673	569
Object	av_target	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
673.      char *av_target = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2795
Status	New

The variable declared in dns_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	670	569
Object	dns_computer	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
670.      char *dns_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2796
Status	New

The variable declared in dns_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	671	569
Object	dns_domain	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
671.      char *dns_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2797
Status	New

The variable declared in dns_tree at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Line	672	569
Object	dns_tree	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
672.      char *dns_tree = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2798
Status	New

The variable declared in nb_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	668	569
Object	nb_computer	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
668.      char *nb_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2799
Status	New

The variable declared in nb_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	669	569
Object	nb_domain	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
669.      char *nb_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2800
Status	New

The variable declared in av_target_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	790	569
Object	av_target_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
790.      char *av_target_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2801
Status	New

The variable declared in dns_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	787	569
Object	dns_computer_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
787.      char *dns_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2802
Status	New

The variable declared in dns_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	788	569
Object	dns_domain_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
788.      char *dns_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2803
Status	New

The variable declared in dns_tree_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	789	569
Object	dns_tree_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
789.      char *dns_tree_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2804
Status	New

The variable declared in nb_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	785	569
Object	nb_computer_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
785.      char *nb_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2805

Status	New

The variable declared in nb_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	786	569
Object	nb_domain_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
786.      char *nb_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2806
Status	New

The variable declared in av_target at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	673	569
Object	av_target	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
673.      char *av_target = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2807
Status	New

The variable declared in dns_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	670	569
Object	dns_computer	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
670.      char *dns_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2808
Status	New

The variable declared in dns_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	671	569
Object	dns_domain	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
671.      char *dns_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2809
Status	New

The variable declared in dns_tree at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	672	569
Object	dns_tree	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
672.      char *dns_tree = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2810
Status	New

The variable declared in nb_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	668	569
Object	nb_computer	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
668.      char *nb_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2811
Status	New

The variable declared in nb_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c

Line	669	569
Object	nb_domain	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
669.      char *nb_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2812
Status	New

The variable declared in av_target_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	790	569
Object	av_target_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
790.      char *av_target_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2813
Status	New

The variable declared in dns_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	787	569
Object	dns_computer_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
787.      char *dns_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2814
Status	New

The variable declared in dns_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	788	569
Object	dns_domain_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
788.      char *dns_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2815
Status	New

The variable declared in dns_tree_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	789	569
Object	dns_tree_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
789.      char *dns_tree_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2816
Status	New

The variable declared in nb_computer_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	785	569
Object	nb_computer_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
785.      char *nb_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2817
Status	New

The variable declared in nb_domain_name at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 777 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	786	569
Object	nb_domain_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
786.      char *nb_domain_name = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2818
Status	New

The variable declared in av_target at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	673	569
Object	av_target	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
673.      char *av_target = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2819
Status	New

The variable declared in dns_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	670	569
Object	dns_computer	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
670.      char *dns_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2820
Status New

The variable declared in dns_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	671	569
Object	dns_domain	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
671.      char *dns_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2821
Status	New

The variable declared in dns_tree at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	672	569
Object	dns_tree	data

Code Snippet

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
672.      char *dns_tree = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2822
Status	New

The variable declared in nb_computer at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	668	569
Object	nb_computer	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
668.      char *nb_computer = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2823
Status	New

The variable declared in nb_domain at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 655 is not initialized when it is used by data at gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c in line 508.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	669	569
Object	nb_domain	data

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_decode_target_info(struct ntlm_ctx *ctx, struct ntlm_buffer *buffer,

```
....
669.      char *nb_domain = NULL;
```

File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
569.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2824
Status	New

The variable declared in av_target_name at gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c in line 755 is not initialized when it is used by data at gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c in line 486.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	768	547
Object	av_target_name	data

Code Snippet

File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c

Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
768.      char *av_target_name = NULL;
```

File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c

Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
547.      buffer.data = calloc(1, buffer.length);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2825
Status	New

The variable declared in dns_computer_name at gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c in line 755 is not initialized when it is used by data at gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c in line 486.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-

	25563-TP.c	25563-TP.c
Line	765	547
Object	dns_computer_name	data

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method int ntlm_process_target_info(struct ntlm_ctx *ctx, bool protect,

```
....
765.      char *dns_computer_name = NULL;
```

File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method int ntlm_encode_target_info(struct ntlm_ctx *ctx, char *nb_computer_name,

```
....
547.      buffer.data = calloc(1, buffer.length);
```

Double Free

Query Path:
CPP\Cx\CPP Medium Threat\Double Free Version:1

Categories

NIST SP 800-53: SI-16 Memory Protection (P1)

Description
Double Free\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1698
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	330	340
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.                    free(spn);
....
340.                        free(spn);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1699
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	340	346
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
340.                        free(spn);
....
346.                        free(spn);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1700
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	330	346
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.                    free(spn);
....
346.                        free(spn);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1701
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	346	353
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
346.                        free(spn);
....
353.                    free(spn);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1702
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	330	353
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.                    free(spn);
....
353.                    free(spn);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1703
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	340	353
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
340.                        free(spn);
....
353.                    free(spn);
```

Double Free\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1704
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	353	358
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
353.                    free(spn);
....
358.            free(spn);
```

Double Free\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1705
Status New

	Source	Destination

File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	346	358
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
346.                        free(spn);
....
358.          free(spn);
```

Double Free\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1706
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	330	358
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.                    free(spn);
....
358.          free(spn);
```

Double Free\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1707
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c

Line	319	358
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
319.                    free(spn);
....
358.            free(spn);
```

Double Free\Path 11:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1708
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	340	358
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
340.                        free(spn);
....
358.            free(spn);
```

Double Free\Path 12:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1709
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	326	336
Object	spn	spn

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
336.                        free(spn);
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1710
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	336	342
Object	spn	spn

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
....
342.                        free(spn);
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1711
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	326	342
Object	spn	spn

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c

Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
342.                        free(spn);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1712
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	342	349
Object	spn	spn

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
342.                        free(spn);
....
349.                    free(spn);
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1713
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	326	349
Object	spn	spn

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
349.                    free(spn);
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1714
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	336	349
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
....
349.                    free(spn);
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1715
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	349	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
349.                    free(spn);
....
354.            free(spn);
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1716
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	342	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
342.                        free(spn);
....
354.            free(spn);
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1717
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	326	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
354.            free(spn);
```

Double Free\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1718
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	315	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
315.                    free(spn);
....
354.            free(spn);
```

Double Free\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1719
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	336	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
....
354.          free(spn);
```

Double Free\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1720
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	326	336
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
336.                        free(spn);
```

Double Free\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1721
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	336	342
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
....
342.                        free(spn);
```

Double Free\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1722
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	326	342
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
342.                        free(spn);
```

Double Free\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1723
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	342	349
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
342.                        free(spn);
....
349.                    free(spn);
```

Double Free\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1724
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	326	349
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
349.                    free(spn);
```

Double Free\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1725
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	336	349
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
....
349.                    free(spn);
```

Double Free\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1726
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	342	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
342.                        free(spn);
....
354.            free(spn);
```

Double Free\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1727
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	349	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
349.                    free(spn);
....
354.            free(spn);
```

Double Free\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1728
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	315	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
315.                    free(spn);
....
354.            free(spn);
```

Double Free\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1729
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	326	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
326.                    free(spn);
....
354.            free(spn);
```

Double Free\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1730
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	336	354
Object	spn	spn

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
336.                        free(spn);
....
354.            free(spn);
```

Double Free\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1731
Status	New

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	786	446
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
786.        free(filename);
```

File Name gwsw@@less-v555-CVE-2022-48624-TP.c

Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1732
Status	New

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	786	446
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v555-CVE-2024-32487-TP.c

Method lglob(filename)

```
....
786.        free(filename);
```

File Name gwsw@@less-v555-CVE-2024-32487-TP.c

Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1733
Status	New

	Source	Destination

File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	786	446
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
786.        free(filename);
```

File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 37:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1734
Status New

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	786	446
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
786.        free(filename);
```

File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1735
Status	New

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	787	446
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v568-CVE-2022-48624-TP.c

Method lglob(filename)

```
....
787.        free(filename);
```

File Name gwsw@@less-v568-CVE-2022-48624-TP.c

Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1736
Status	New

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	787	446
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v568-CVE-2024-32487-TP.c

Method lglob(filename)

```
....
787.        free(filename);
```

File Name gwsw@@less-v568-CVE-2024-32487-TP.c

Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1737
Status	New

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	787	446
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v580-CVE-2022-48624-TP.c

Method lglob(filename)

```
....
787.        free(filename);
```

File Name gwsw@@less-v580-CVE-2022-48624-TP.c

Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1738
Status	New

	Source	Destination

File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	787	446
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
787.        free(filename);
```

File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method fcomplete(s)

```
....
446.        free(fpat);
```

Double Free\Path 42:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1739
Status New

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	791	451
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
791.        free(filename);
```

File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1740
Status	New

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	791	451
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v590-CVE-2024-32487-TP.c

Method lglob(filename)

```
....
791.        free(filename);
```

File Name gwsw@@less-v590-CVE-2024-32487-TP.c

Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1741
Status	New

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	792	451
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v594-CVE-2022-48624-TP.c

Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v594-CVE-2022-48624-TP.c

Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1742
Status	New

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	792	451
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v594-CVE-2024-32487-TP.c

Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v594-CVE-2024-32487-TP.c

Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1743
Status	New

	Source	Destination

File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	792	451
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 47:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1744
Status New

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	792	451
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1745
Status	New

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	792	451
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1746
Status	New

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	792	451
Object	filename	fpat

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v605-CVE-2024-32487-TP.c

Method fcomplete(s)

```
....
451.        free(fpat);
```

Double Free\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=1747
Status	New

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	792	451
Object	filename	fpat

Code Snippet

File Name gwsw@@less-v609-CVE-2024-32487-TP.c

Method lglob(filename)

```
....
792.        free(filename);
```

File Name gwsw@@less-v609-CVE-2024-32487-TP.c

Method fcomplete(s)

```
....
451.        free(fpat);
```

Wrong Size t Allocation

Query Path:

CPP\Cx\CPP Integer Overflow\Wrong Size t Allocation Version:0

Description

Wrong Size t Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=348

Status	New

The function full_string_len in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c at line 793 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	821	821
Object	full_string_len	full_string_len

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
821.          char *attr_string = malloc(full_string_len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=349
Status	New

The function l in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c at line 263 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	338	338
Object	l	l

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
338.                  name->data.server.spn = malloc(l);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=350
Status	New

The function full_string_len in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c at line 852 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	880	880
Object	full_string_len	full_string_len

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
880.          char *attr_string = malloc(full_string_len);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=351
Status	New

The function l in gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c at line 259 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	334	334
Object	l	l

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
334.                  name->data.server.spn = malloc(l);
```

Wrong Size t Allocation\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=352
Status	New

The function full_string_len in gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c at line 848 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	876	876
Object	full_string_len	full_string_len

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
876.          char *attr_string = malloc(full_string_len);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=353
Status	New

The function l in gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c at line 259 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	334	334
Object	l	l

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
334.                  name->data.server.spn = malloc(l);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=354
Status	New

The function full_string_len in gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c at line 848 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	876	876
Object	full_string_len	full_string_len

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
876.          char *attr_string = malloc(full_string_len);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=355
Status	New

The function i in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c at line 387 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	411	411
Object	i	i

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
411.          copied_attrs[i].attr_value.value =
malloc(src[i].attr_value.length);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=356
Status	New

The function i in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c at line 436 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	460	460
Object	i	i

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
460.          copied_attrs[i].attr_value.value =
malloc(src[i].attr_value.length);
```

Wrong Size t Allocation\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=357
Status	New

The function i in gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c at line 432 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	456	456
Object	i	i

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
456.          copied_attrs[i].attr_value.value =
malloc(src[i].attr_value.length);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=358
Status	New

The function i in gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c at line 432 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	456	456
Object	i	i

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
456.          copied_attrs[i].attr_value.value =
malloc(src[i].attr_value.length);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=359
Status	New

The function attrs_count in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c at line 387 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	398	398
Object	attrs_count	attrs_count

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method	int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
398.      copied_attrs = calloc(attrs_count + 1, /* +1 for terminator
entry */
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=360
Status	New

The function attrs_count in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c at line 436 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	447	447
Object	attrs_count	attrs_count

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method	int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
447.      copied_attrs = calloc(attrs_count + 1, /* +1 for terminator
entry */
```

Wrong Size t Allocation\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=361
Status	New

The function attrs_count in gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c at line 432 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	443	443

Object	attrs_count	attrs_count

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
443.      copied_attrs = calloc(attrs_count + 1, /* +1 for terminator
entry */
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=362
Status	New

The function attrs_count in gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c at line 432 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	443	443
Object	attrs_count	attrs_count

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method int gssntlm_copy_attrs(const struct gssntlm_name_attribute *src,

```
....
443.      copied_attrs = calloc(attrs_count + 1, /* +1 for terminator
entry */
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=363
Status	New

The function inlen in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c at line 462 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-

	25563-TP.c	25563-TP.c
Line	472	472
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=364
Status	New

The function inlen in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c at line 462 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	472	472
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=365
Status	New

The function inlen in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c at line 462 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination

File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	472	472
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 19:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=366
Status New

The function inlen in gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c at line 462 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	472	472
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 20:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=367
Status New

The function inlen in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c at line 440 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	450	450
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=368
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c at line 440 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Line	450	450
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=369
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c at line 440 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Line	450	450
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=370
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c at line 440 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Line	450	450
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=371
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c at line 439 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Line	449	449
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 25:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=372
Status New

The function inlen in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c at line 439 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Line	449	449
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 26:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=373
Status New

The function inlen in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c at line 439 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Line	449	449
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=374
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c at line 439 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Line	449	449
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=375
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c at line 442 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Line	452	452
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
452.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=376
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c at line 442 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Line	452	452
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
452.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=377
Status	New

The function inlen in gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c at line 444 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Line	454	454
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
454.        out = malloc(inlen * 2 + 1);
```

Wrong Size t Allocation\Path 31:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=378
Status New

The function inlen in gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c at line 444 assigns an incorrectly calculated size to a buffer, resulting in a mismatch between the value being written and the size of the buffer it is being written into.

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Line	454	454
Object	inlen	inlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
454.        out = malloc(inlen * 2 + 1);
```

Use of Uninitialized Variable

Query Path:
CPP\Cx\CPP Medium Threat\Use of Uninitialized Variable Version:0

Categories

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

Description

Use of Uninitialized Variable\Path 1:

Severity Medium
Result State To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2764
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	509	537
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_duplicate_name(uint32_t *minor_status,

```
....
509.      uint32_t retmaj;
....
537.      if (retmaj) {
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2765
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	662	707
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
662.      uint32_t retmaj;
....
707.      if (retmaj) {
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2766
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	567	595
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_duplicate_name(uint32_t *minor_status,

```
....
567.      uint32_t retmaj;
....
595.      if (retmaj) {
```

Use of Uninitialized Variable\Path 4:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2767
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	721	766
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
721.      uint32_t retmaj;
....
766.      if (retmaj) {
```

Use of Uninitialized Variable\Path 5:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2768
Status New

	Source	Destination

File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	563	591
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_duplicate_name(uint32_t *minor_status,

```
....
563.      uint32_t retmaj;
....
591.      if (retmaj) {
```

Use of Uninitialized Variable\Path 6:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2769
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	717	762
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
717.      uint32_t retmaj;
....
762.      if (retmaj) {
```

Use of Uninitialized Variable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2770
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c

Line	563	591
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_duplicate_name(uint32_t *minor_status,

```
....
563.      uint32_t retmaj;
....
591.      if (retmaj) {
```

Use of Uninitialized Variable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2771
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	717	762
Object	retmaj	retmaj

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_localname(uint32_t *minor_status,

```
....
717.      uint32_t retmaj;
....
762.      if (retmaj) {
```

Use of Uninitialized Variable\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2772
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	268	359
Object	retmaj	retmaj

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
268.      uint32_t retmaj;
....
359.      if (retmaj != GSS_S_COMPLETE) {
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2773
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	270	408
Object	retmaj	retmaj

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
270.      uint32_t retmaj;
....
408.      if (retmaj != GSS_S_COMPLETE) {
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2774
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	266	404
Object	retmaj	retmaj

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c

Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
266.      uint32_t retmaj;
....
404.      if (retmaj != GSS_S_COMPLETE) {
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2775
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	266	404
Object	retmaj	retmaj

Code Snippet

File Name	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method	uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
266.      uint32_t retmaj;
....
404.      if (retmaj != GSS_S_COMPLETE) {
```

Char Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Char Overflow 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)

Description

Char Overflow\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=379
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 789 of gwsw@@less-v555-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	gwsw@@less-v555-CVE-2022-46663-TP.c	gwsw@@less-v555-CVE-2022-46663-TP.c
Line	853	853
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v555-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
853.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=380
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 789 of gwsw@@less-v564-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-46663-TP.c	gwsw@@less-v564-CVE-2022-46663-TP.c
Line	853	853
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v564-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
853.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=381
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 823 of gwsw@@less-v568-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	gwsw@@less-v568-CVE-2022-46663-TP.c	gwsw@@less-v568-CVE-2022-46663-TP.c
Line	887	887
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v568-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
887.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=382
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 830 of gwsw@@less-v580-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-46663-TP.c	gwsw@@less-v580-CVE-2022-46663-TP.c
Line	894	894
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v580-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
894.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=383
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 840 of gwsw@@less-v590-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	gwsw@@less-v590-CVE-2022-46663-TP.c	gwsw@@less-v590-CVE-2022-46663-TP.c
Line	904	904
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v590-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
904.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=384
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 898 of gwsw@@less-v594-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	gwsw@@less-v594-CVE-2022-46663-TP.c	gwsw@@less-v594-CVE-2022-46663-TP.c
Line	962	962
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v594-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
962.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=385
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 919 of gwsw@@less-v600-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	gwsw@@less-v600-CVE-2022-46663-TP.c	gwsw@@less-v600-CVE-2022-46663-TP.c
Line	983	983
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v600-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
983.                    mbc_buf[mbc_buf_index++] = c;
```

Char Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=386
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 919 of gwsw@@less-v605-CVE-2022-46663-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-46663-TP.c	gwsw@@less-v605-CVE-2022-46663-TP.c
Line	983	983
Object	AssignExpr	AssignExpr

Code Snippet
File Name gwsw@@less-v605-CVE-2022-46663-TP.c
Method pappend(c, pos)

```
....
983.                    mbc_buf[mbc_buf_index++] = c;
```

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=1000032&projectid=26&pathid=387
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 579 of h2o@@h2o-newest-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	611	611
Object	AssignExpr	AssignExpr

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
611.                    i += l;
```

Integer Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=388
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 579 of h2o@@h2o-newest-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	627	627
Object	AssignExpr	AssignExpr

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
627.                        i += l;
```

Integer Overflow\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=389
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 579 of h2o@@h2o-newest-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	644	644
Object	AssignExpr	AssignExpr

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method sds sdscatfmt(sds s, char const *fmt, ...) {

```
....
644.                        i += l;
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=390
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 712 of h2o@@h2o-newest-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	717	717
Object	AssignExpr	AssignExpr

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method void sdsrange(sds s, int start, int end) {

```
....
717.            start = len+start;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=391
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 712 of h2o@@h2o-newest-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	721	721
Object	AssignExpr	AssignExpr

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method void sdsrange(sds s, int start, int end) {

```
....
721.          end = len+end;
```

Integer Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=392
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 712 of h2o@@h2o-newest-CVE-2021-21309-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	729	729
Object	AssignExpr	AssignExpr

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method void sdsrange(sds s, int start, int end) {

```
....
729.              end = len-1;
```

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=1000032&projectid=26&pathid=2587
Status	New

The variable declared in null at HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	546	582
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
582.              layout = audio_config->in.channel_layout;
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2588
Status	New

The variable declared in null at HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	546	566
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
566.          samplerate = audio_config->in.samplerate;
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2589
Status	New

The variable declared in null at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c in line 541 is not initialized when it is used by in at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c in line 541.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	550	586
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
550.      hb_audio_config_t * audio_config = NULL;
....
586.              layout = audio_config->in.channel_layout;
```

NULL Pointer Dereference\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2590
Status	New

The variable declared in null at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c in line 541 is not initialized when it is used by in at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c in line 541.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	550	570
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
550.      hb_audio_config_t * audio_config = NULL;
....
570.          samplerate = audio_config->in.samplerate;
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2591
Status	New

The variable declared in null at HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	546	582
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
582.              layout = audio_config->in.channel_layout;
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2592
Status	New

The variable declared in null at HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c

Line	546	566
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
566.          samplerate = audio_config->in.samplerate;
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2593
Status	New

The variable declared in null at HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	546	582
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
582.              layout = audio_config->in.channel_layout;
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2594
Status	New

The variable declared in null at HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination

File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	546	566
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
566.          samplerate = audio_config->in.samplerate;
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2595
Status	New

The variable declared in null at HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	546	582
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
582.              layout = audio_config->in.channel_layout;
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2596
Status	New

The variable declared in null at HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	546	566
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
566.          samplerate = audio_config->in.samplerate;
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2597
Status	New

The variable declared in null at HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	546	582
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
582.              layout = audio_config->in.channel_layout;
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2598
Status	New

The variable declared in null at HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c in line 537 is not initialized when it is used by in at HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c in line 537.

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	546	566
Object	null	in

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method void hb_sanitize_audio_settings(const hb_title_t * title,

```
....
546.      hb_audio_config_t * audio_config = NULL;
....
566.          samplerate = audio_config->in.samplerate;
```

NULL Pointer Dereference\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2599
Status New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by pv at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1019
Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

NULL Pointer Dereference\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2600

Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1588
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1588.                  pv->param.gop.b_pyramid ? "pyramid" : "off");
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2601
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1534
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1534.          option2->LookAheadDepth = pv-
>param.codingOption2.LookAheadDepth;
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2602
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1474
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.       pv->is_sys_mem          = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1474.       if (pv->param.videoParam->mfx.CodecId == MFX_CODEC_AVC)
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2603
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1447
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1447.          pv->param.videoParam->mfx.RateControlMethod ==
MFX_RATECONTROL_LA)
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2604
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1411
Object	0	qsv_info

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1411.      if (pv->qsv_info->implementation & MFX_IMPL_HARDWARE_ANY)
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2605
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by pv at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1573

Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1573.             pv->is_sys_mem ? "encode-only" : "full QSV",
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2606
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by pv at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1540
Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1540.      if (pv->is_sys_mem)
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2607
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination

File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	213
Object	0	qsv_info

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
213.      if (pv->qsv_info->capabilities & HB_QSV_CAP_OPTION2_BREFTYPE)
```

NULL Pointer Dereference\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2608
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	167
Object	0	qsv_info

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
167.      if (!(pv->qsv_info->capabilities & HB_QSV_CAP_B_REF_PYRAMID))
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2609
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	216
Object	0	param

Code Snippet

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
216.          if (pv->param.gop.b_pyramid)
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2610
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-	HandBrake@@HandBrake-1.3.2-CVE-

	2022-38890-FP.c	2022-38890-FP.c
Line	1019	267
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
267.              if (pv->param.videoParam->mfx.NumRefFrame)
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2611
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	254
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
254.              if (pv->param.videoParam->mfx.GopPicSize)
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2612
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	274
Object	0	param

Code Snippet

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
274.          else if (pv->param.videoParam->mfx.GopRefDist == 0 ||
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2613
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-	HandBrake@@HandBrake-1.3.2-CVE-

	2022-38890-FP.c	2022-38890-FP.c
Line	1019	275
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
275.                    pv->param.videoParam->mfx.GopRefDist ==
pyramid_ref_dist)
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2614
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	243
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
243.          if (pv->param.gop.b_pyramid)
```

NULL Pointer Dereference\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2615
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	238
Object	0	param

Code Snippet

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
238.          while (pv->param.videoParam->mfx.GopRefDist >
pyramid_ref_dist)
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2616
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination

File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	208
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
208.      if (pv->param.gop.b_pyramid < 0)
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2617
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	196
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
196.      else if (pv->param.videoParam->mfx.CodecId == MFX_CODEC_HEVC)
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2618
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	184
Object	0	param

Code Snippet

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
184.      else if (pv->param.videoParam->mfx.CodecId == MFX_CODEC_AVC)
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2619
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-	HandBrake@@HandBrake-1.3.2-CVE-

	2022-38890-FP.c	2022-38890-FP.c
Line	1019	178
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
178.      else if (pv->param.videoParam->mfx.GopRefDist &&
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2620
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	179
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
179.                pv->param.videoParam->mfx.GopRefDist <= 2)
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2621
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	172
Object	0	param

Code Snippet

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
172.      else if (pv->param.videoParam->mfx.GopPicSize &&
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2622
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by param at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 161.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-	HandBrake@@HandBrake-1.3.2-CVE-

	2022-38890-FP.c	2022-38890-FP.c
Line	1019	173
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
173.               pv->param.videoParam->mfx.GopPicSize <= 3)
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2623
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014 is not initialized when it is used by pv at HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c in line 1014.

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Line	1019	1360
Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1019.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1360.      if (!pv->is_sys_mem)
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2624
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by pv at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1040
Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2625
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by param at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1623
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1623.                 pv->param.gop.b_pyramid ? "pyramid" : "off");
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2626
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by param at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1569
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1569.          option2->LookAheadDepth = pv-
>param.codingOption2.LookAheadDepth;
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2627
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by param at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1509
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.       pv->is_sys_mem          = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1509.       if (pv->param.videoParam->mfx.CodecId == MFX_CODEC_AVC)
```

NULL Pointer Dereference\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2628
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by param at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1482
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.       pv->is_sys_mem          = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1482.           pv->param.videoParam->mfx.RateControlMethod ==
MFX_RATECONTROL_LA)
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2629
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Line	1040	1442
Object	0	qsv_info

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1442.          hb_error("encqsvInit: MFXInit failed (%d) with
implementation %d", err, pv->qsv_info->implementation);
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2630
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1446
Object	0	qsv_info

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1446.      if (pv->qsv_info->implementation & MFX_IMPL_HARDWARE_ANY)
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2631
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by pv at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1608
Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1608.             pv->is_sys_mem ? "encode-only" : "full QSV",
```

NULL Pointer Dereference\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2632
Status New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by pv at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	1575
Object	0	pv

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
....
1575.      if (pv->is_sys_mem)
```

NULL Pointer Dereference\Path 47:

Severity Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2633
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 158.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	210
Object	0	qsv_info

Code Snippet

File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
210.      if (pv->qsv_info->capabilities & HB_QSV_CAP_OPTION2_BREFTYPE)
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2634
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by qsv_info at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 158.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	164
Object	0	qsv_info

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
164.      if (!(pv->qsv_info->capabilities & HB_QSV_CAP_B_REF_PYRAMID))
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2635
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by param at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 158.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	213
Object	0	param

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
213.          if (pv->param.gop.b_pyramid)
```

NULL Pointer Dereference\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2636
Status	New

The variable declared in 0 at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 1035 is not initialized when it is used by param at HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c in line 158.

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c
Line	1040	264
Object	0	param

Code Snippet

File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Method int encqsvInit(hb_work_object_t *w, hb_job_t *job)

```
....
1040.      pv->is_sys_mem         = hb_qsv_full_path_is_enabled(job) ? 0
: 1; // TODO: re-implement QSV VPP filtering support
```

File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2022-38890-FP.c

Method static void qsv_handle_breftype(hb_work_private_t *pv)

```
....
264.              if (pv->param.videoParam->mfx.NumRefFrame)
```

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=1000032&projectid=26&pathid=3062
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-

	25563-TP.c	25563-TP.c
Line	345	345
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
345.        out[outlen] = '\0';
```

Unchecked Array Index\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3063
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	480	480
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
480.        out[outlen] = '\0';
```

Unchecked Array Index\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3064
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	345	345
Object	outlen	outlen

Code Snippet

File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method	static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
345.      out[outlen] = '\0';
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3065
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	480	480
Object	outlen	outlen

Code Snippet

File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method	static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
480.      out[outlen] = '\0';
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3066
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	345	345
Object	outlen	outlen

Code Snippet

File Name	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method	static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
345.      out[outlen] = '\0';
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3067
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	480	480
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
480.        out[outlen] = '\0';
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3068
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	345	345
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_ucs2_str_hdr(struct ntlm_ctx *ctx,

```
....
345.        out[outlen] = '\0';
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3069
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	480	480
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
480.        out[outlen] = '\0';
```

Unchecked Array Index\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3070
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.        out[outlen] = '\0';
```

Unchecked Array Index\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3071
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	458	458

Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
458.      out[outlen] = '\0';
```

Unchecked Array Index\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3072
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.      out[outlen] = '\0';
```

Unchecked Array Index\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3073
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Line	458	458
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
458.        out[outlen] = '\0';
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3074
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.        out[outlen] = '\0';
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3075
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Line	458	458
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
458.        out[outlen] = '\0';
```

Unchecked Array Index\Path 15:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3076
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	308	308
Object	HOST_NAME_MAX	HOST_NAME_MAX

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
308.          hostname[HOST_NAME_MAX] = '\0';
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3077
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	836	836
Object	offset	offset

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
836.          attr_string[offset] = 0;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3078
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.        out[outlen] = '\0';
```

Unchecked Array Index\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3079
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Line	458	458
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
458.        out[outlen] = '\0';
```

Unchecked Array Index\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3080
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Line	323	323

Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.        out[outlen] = '\0';
```

Unchecked Array Index\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3081
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Line	457	457
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
457.        out[outlen] = '\0';
```

Unchecked Array Index\Path 21:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3082
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.        out[outlen] = '\0';
```

Unchecked Array Index\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3083
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Line	457	457
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
457.        out[outlen] = '\0';
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3084
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.        out[outlen] = '\0';
```

Unchecked Array Index\Path 24:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3085
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Line	457	457
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
457.      out[outlen] = '\0';
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3086
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	334	334
Object	MAXHOSTNAMELEN	MAXHOSTNAMELEN

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
334.              hostname[HOST_NAME_MAX] = '\0';
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3087
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	895	895
Object	offset	offset

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
895.          attr_string[offset] = 0;
```

Unchecked Array Index\Path 27:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3088
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Line	323	323
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
323.      out[outlen] = '\0';
```

Unchecked Array Index\Path 28:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3089
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Line	457	457

Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
457.      out[outlen] = '\0';
```

Unchecked Array Index\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3090
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Line	328	328
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
328.          out[outlen] = '\0';
```

Unchecked Array Index\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3091
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Line	460	460
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25563-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
460.        out[outlen] = '\0';
```

Unchecked Array Index\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3092
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Line	328	328
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
328.            out[outlen] = '\0';
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3093
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Line	460	460
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
460.        out[outlen] = '\0';
```

Unchecked Array Index\Path 33:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3094
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	330	330
Object	MAXHOSTNAMELEN	MAXHOSTNAMELEN

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.              hostname[HOST_NAME_MAX] = '\0';
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3095
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Line	891	891
Object	offset	offset

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.2.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
891.          attr_string[offset] = 0;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3096
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Line	329	329
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
329.              out[outlen] = '\0';
```

Unchecked Array Index\Path 36:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3097
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Line	462	462
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25563-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
462.      out[outlen] = '\0';
```

Unchecked Array Index\Path 37:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3098
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Line	329	329

Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_u16l_str_hdr(struct ntlm_ctx *ctx,

```
....
329.              out[outlen] = '\0';
```

Unchecked Array Index\Path 38:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3099
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Line	462	462
Object	outlen	outlen

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25564-FP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
462.      out[outlen] = '\0';
```

Unchecked Array Index\Path 39:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3100
Status New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	330	330
Object	MAXHOSTNAMELEN	MAXHOSTNAMELEN

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_import_name_by_mech(uint32_t *minor_status,

```
....
330.              hostname[HOST_NAME_MAX] = '\0';
```

Unchecked Array Index\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3101
Status	New

	Source	Destination
File	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c	gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Line	891	891
Object	offset	offset

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.3.0-CVE-2023-25566-FP.c
Method uint32_t gssntlm_inquire_name(uint32_t *minor_status,

```
....
891.          attr_string[offset] = 0;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3102
Status	New

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1635	1635
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parser_parse_vps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
1635.      parser->vps[vps->id] = *vps;
```

Unchecked Array Index\Path 42:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3103
Status	New

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1805	1805
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parser_parse_sps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
1805.       parser->sps[sps->id] = *sps;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3104
Status	New

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	2410	2410
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parser_parse_pps (GstH265Parser * parser,

```
....
2410.       parser->pps[pps->id] = *pps;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3105
Status	New

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	3045	3045
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parser_update_vps (GstH265Parser * parser, GstH265VPS * vps)

```
....
3045.    parser->vps[vps->id] = *vps;
```

Unchecked Array Index\Path 45:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3106
Status New

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	3086	3086
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parser_update_sps (GstH265Parser * parser, GstH265SPS * sps)

```
....
3086.    parser->sps[sps->id] = *sps;
```

Unchecked Array Index\Path 46:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3107
Status New

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	3132	3132

Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parser_update_pps (GstH265Parser * parser, GstH265PPS * pps)

```
....
3132.    parser->pps[pps->id] = *pps;
```

Unchecked Array Index\Path 47:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3108
Status New

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1635	1635
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method gst_h265_parser_parse_vps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
1635.      parser->vps[vps->id] = *vps;
```

Unchecked Array Index\Path 48:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3109
Status New

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1805	1805
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method gst_h265_parser_parse_sps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
1805.      parser->sps[sps->id] = *sps;
```

Unchecked Array Index\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3110
Status	New

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	2410	2410
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method gst_h265_parser_parse_pps (GstH265Parser * parser,

```
....
2410.      parser->pps[pps->id] = *pps;
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3111
Status	New

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	3045	3045
Object	id	id

Code Snippet
File Name GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method gst_h265_parser_update_vps (GstH265Parser * parser, GstH265VPS * vps)

```
....
3045.    parser->vps[vps->id] = *vps;
```

Potential Off by One Error in Loops

Query Path:

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=1000032&projectid=26&pathid=2492
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 389 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	396	396
Object	<=	<=

Code Snippet
File Name GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method gst_h265_parse_sub_layer_hrd_parameters (GstH265SubLayerHRDParams * sub_hrd,

```
....
396.     for (i = 0; i <= CpbCnt; i++) {
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2493
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	457	457
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parse_hrd_parameters (GstH265HRDParams * hrd, NalReader * nr,

```
....
457.    for (i = 0; i <= maxNumSubLayersMinus1; 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=1000032&projectid=26&pathid=2494
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 770 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	810	810
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_short_term_ref_pic_sets (GstH265ShortTermRefPicSet *

```
....
810.      for (j = 0; j <= RefRPS->NumDeltaPocs; j++) {
```

Potential Off by One Error in Loops\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2495
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 916 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	926	926
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_ref_pic_list_modification (GstH265SliceHdr * slice,

```
....
926.      for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2496
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 916 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	934	934
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_ref_pic_list_modification (GstH265SliceHdr * slice,

```
....
934.        for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2497
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	966	966
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c

Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
966.    for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2498
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	970	970
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
970.      for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2499
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	973	973
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
973.    for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2500
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	986	986
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
986.      for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2501
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	989	989
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
989.        for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2502
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	992	992
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
992.      for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2503
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 1013 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1053	1053
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_buffering_period (GstH265Parser * parser,

```
....
1053.         for (i = 0; i <= hrd->cpb_cnt_minus1[i]; i++) {
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2504
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 1013 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1065	1065
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_buffering_period (GstH265Parser * parser,

```
....
1065.         for (i = 0; i <= hrd->cpb_cnt_minus1[i]; i++) {
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2505
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 1085 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1148	1148
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_pic_timing (GstH265Parser * parser,

```
....
1148.          for (i = 0; i <= tim->num_decoding_units_minus1; i++) {
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2506
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 1652 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1695	1695
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parse_vps (GstH265NalUnit * nalu, GstH265VPS * vps)

```
....
1695.      for (i = 0; i <= (vps->max_sub_layers_minus1 - 1); i++) {
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2507
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 1652 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1714	1714
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parse_vps (GstH265NalUnit * nalu, GstH265VPS * vps)

```
....
1714.       for (j = 0; j <= vps->max_layer_id; j++) {
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2508
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 1824 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	1889	1889
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_parse_sps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
1889.       for (i = 0; i <= (sps->max_sub_layers_minus1 - 1); i++) {
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2509
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 2110 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	2284	2284
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c

Method	gst_h265_parse_pps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
2284.            i <= pps-
>pps_extension_params.chroma_qp_offset_list_len_minus1;
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2510
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c at line 2914 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Line	2936	2936
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.19.90-CVE-2023-40476-TP.c
Method	gst_h265_sei_copy (GstH265SEIMessage * dst_sei,

```
....
2936.        for (i = 0; i <= dst_pic_timing->num_decoding_units_minus1;
i++) {
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2511
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 389 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	396	396
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parse_sub_layer_hrd_parameters (GstH265SubLayerHRDParams * sub_hrd,

```
....
396.    for (i = 0; i <= CpbCnt; i++) {
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2512
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	457	457
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parse_hrd_parameters (GstH265HRDParams * hrd, NalReader * nr,

```
....
457.    for (i = 0; i <= maxNumSubLayersMinus1; i++) {
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2513
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 770 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	810	810
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_short_term_ref_pic_sets (GstH265ShortTermRefPicSet *

```
....
810.      for (j = 0; j <= RefRPS->NumDeltaPocs; j++) {
```

Potential Off by One Error in Loops\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2514
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 916 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	926	926
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_ref_pic_list_modification (GstH265SliceHdr * slice,

```
....
926.      for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2515
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 916 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	934	934
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c

Method	gst_h265_slice_parse_ref_pic_list_modification (GstH265SliceHdr * slice,

```
....
934.        for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2516
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	966	966
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
966.    for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2517
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	970	970
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c

Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
970.      for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2518
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	973	973
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
973.    for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2519
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	986	986
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
986.      for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2520
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	989	989
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
989.        for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2521
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 948 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	992	992
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
992.      for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2522
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 1013 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1053	1053
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_buffering_period (GstH265Parser * parser,

```
....
1053.         for (i = 0; i <= hrd->cpb_cnt_minus1[i]; i++) {
```

Potential Off by One Error in Loops\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2523
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 1013 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1065	1065
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_buffering_period (GstH265Parser * parser,

```
....
1065.         for (i = 0; i <= hrd->cpb_cnt_minus1[i]; i++) {
```

Potential Off by One Error in Loops\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2524
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 1085 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1148	1148
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_pic_timing (GstH265Parser * parser,

```
....
1148.           for (i = 0; i <= tim->num_decoding_units_minus1; i++) {
```

Potential Off by One Error in Loops\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2525
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 1652 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1695	1695
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parse_vps (GstH265NalUnit * nalu, GstH265VPS * vps)

```
....
1695.       for (i = 0; i <= (vps->max_sub_layers_minus1 - 1); i++) {
```

Potential Off by One Error in Loops\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2526
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 1652 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1714	1714
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parse_vps (GstH265NalUnit * nalu, GstH265VPS * vps)

```
....
1714.       for (j = 0; j <= vps->max_layer_id; j++) {
```

Potential Off by One Error in Loops\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2527
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 1824 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	1889	1889
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c

Method	gst_h265_parse_sps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
1889.      for (i = 0; i <= (sps->max_sub_layers_minus1 - 1); i++) {
```

Potential Off by One Error in Loops\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2528
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 2110 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	2284	2284
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Method	gst_h265_parse_pps (GstH265Parser * parser, GstH265NalUnit * nalu,

```
....
2284.            i <= pps->pps_extension_params.chroma_qp_offset_list_len_minus1;
```

Potential Off by One Error in Loops\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2529
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c at line 2914 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c
Line	2936	2936
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.20.2-CVE-2023-40476-TP.c

Method	gst_h265_sei_copy (GstH265SEIMessage * dst_sei,

```
....
2936.         for (i = 0; i <= dst_pic_timing->num_decoding_units_minus1;
i++) {
```

Potential Off by One Error in Loops\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2530
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 389 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	396	396
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_parse_sub_layer_hrd_parameters (GstH265SubLayerHRDParams * sub_hrd,

```
....
396.     for (i = 0; i <= CpbCnt; i++) {
```

Potential Off by One Error in Loops\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2531
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 416 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	457	457
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_parse_hrd_parameters (GstH265HRDParams * hrd, NalReader * nr,

```
....
457.    for (i = 0; i <= maxNumSubLayersMinus1; i++) {
```

Potential Off by One Error in Loops\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2532
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 772 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	812	812
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_short_term_ref_pic_sets (GstH265ShortTermRefPicSet *

```
....
812.      for (j = 0; j <= RefRPS->NumDeltaPocs; j++) {
```

Potential Off by One Error in Loops\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2533
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 918 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	928	928
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c

Method	gst_h265_slice_parse_ref_pic_list_modification (GstH265SliceHdr * slice,

```
....
928.      for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2534
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 918 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	936	936
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_ref_pic_list_modification (GstH265SliceHdr * slice,

```
....
936.        for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2535
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 950 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	968	968
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c

Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
968.    for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2536
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 950 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	972	972
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
972.      for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2537
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 950 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	975	975
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
975.    for (i = 0; i <= slice->num_ref_idx_l0_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2538
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 950 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	988	988
Object	<=	<=

Code Snippet

File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
988.      for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2539
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 950 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	991	991
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
991.        for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++)
```

Potential Off by One Error in Loops\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2540
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 950 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	994	994
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_slice_parse_pred_weight_table (GstH265SliceHdr * slice, NalReader * nr)

```
....
994.      for (i = 0; i <= slice->num_ref_idx_l1_active_minus1; i++) {
```

Potential Off by One Error in Loops\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2541
Status	New

The buffer allocated by <= in GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c at line 1015 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Line	1055	1055
Object	<=	<=

Code Snippet	
File Name	GStreamer@@gstreamer-1.21.1-CVE-2023-40476-TP.c
Method	gst_h265_parser_parse_buffering_period (GstH265Parser * parser,

```
....
1055.         for (i = 0; i <= hrd->cpb_cnt_minus1[i]; i++) {
```

Unchecked Return Value

Query Path:
CPP\Cx\CPP Low Visibility\Unchecked Return Value Version:1

Categories

NIST SP 800-53: SI-11 Error Handling (P2)

Description

Unchecked Return Value\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2402
Status	New

The lglob method calls the sprintf function, at line 613 of gwsw@@less-v555-CVE-2022-48624-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	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	655	655
Object	sprintf	sprintf

Code Snippet	
File Name	gwsw@@less-v555-CVE-2022-48624-TP.c
Method	lglob(filename)

```
....
655.                     sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2403
Status	New

The lglob method calls the sprintf function, at line 613 of gwsw@@less-v555-CVE-2024-32487-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	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	655	655
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2404
Status New

The lglob method calls the sprintf function, at line 613 of gwsw@@less-v564-CVE-2022-48624-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	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	655	655
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=2405
Status	New

The lglob method calls the sprintf function, at line 613 of gwsw@@less-v564-CVE-2024-32487-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	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	655	655
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2406
Status	New

The lglob method calls the sprintf function, at line 614 of gwsw@@less-v568-CVE-2022-48624-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	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	656	656
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 6:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2407
Status	New

The lglob method calls the sprintf function, at line 614 of gwsw@@less-v568-CVE-2024-32487-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	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	656	656
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2408
Status	New

The lglob method calls the sprintf function, at line 614 of gwsw@@less-v580-CVE-2022-48624-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	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	656	656
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v580-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2409
Status	New

The lglob method calls the sprintf function, at line 614 of gwsw@@less-v580-CVE-2024-32487-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	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	656	656
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2410
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v590-CVE-2022-48624-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	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2411
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v590-CVE-2024-32487-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	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2412
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v594-CVE-2022-48624-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	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet	
File Name	gwsw@@less-v594-CVE-2022-48624-TP.c
Method	lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2413
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v594-CVE-2024-32487-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	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet	
File Name	gwsw@@less-v594-CVE-2024-32487-TP.c
Method	lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2414
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v600-CVE-2022-48624-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	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	660	660

Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2415
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v600-CVE-2024-32487-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	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2416
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v605-CVE-2022-48624-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	gwsw@@less-v605-CVE-2022-48624-	gwsw@@less-v605-CVE-2022-48624-

	TP.c	TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2417
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v605-CVE-2024-32487-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	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2418
Status	New

The lglob method calls the sprintf function, at line 618 of gwsw@@less-v609-CVE-2024-32487-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	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	660	660
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2419
Status New

The lglob method calls the sprintf function, at line 595 of gwsw@@less-v624-CVE-2024-32487-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	gwsw@@less-v624-CVE-2024-32487-TP.c	gwsw@@less-v624-CVE-2024-32487-TP.c
Line	636	636
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v624-CVE-2024-32487-TP.c
Method public char * lglob(char *filename)

```
....
636.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2420
Status New

The lglob method calls the sprintf function, at line 595 of gwsw@@less-v634-CVE-2024-32487-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	gwsw@@less-v634-CVE-2024-32487-TP.c	gwsw@@less-v634-CVE-2024-32487-TP.c
Line	636	636
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v634-CVE-2024-32487-TP.c
Method public char * lglob(char *filename)

```
....
636.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2421
Status	New

The lglob method calls the sprintf function, at line 595 of gwsw@@less-v644-CVE-2024-32487-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	gwsw@@less-v644-CVE-2024-32487-TP.c	gwsw@@less-v644-CVE-2024-32487-TP.c
Line	636	636
Object	sprintf	sprintf

Code Snippet
File Name gwsw@@less-v644-CVE-2024-32487-TP.c
Method public char * lglob(char *filename)

```
....
636.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26

	&pathid=2422
Status	New

The source_audio_track_used method calls the snprintf function, at line 387 of HandBrake@@HandBrake-1.3.2-CVE-2023-35853-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	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	391	391
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method static hb_dict_t * source_audio_track_used(hb_dict_t *track_dict, int track)

```
....
391.      snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2423
Status	New

The add_audio_for_lang method calls the snprintf function, at line 632 of HandBrake@@HandBrake-1.3.2-CVE-2023-35853-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	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method static void add_audio_for_lang(hb_value_array_t *list, const hb_dict_t *preset,

```
....
644.          snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 23:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2424
Status	New

The source_audio_track_used method calls the snprintf function, at line 391 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-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	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	395	395
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method static hb_dict_t * source_audio_track_used(hb_dict_t *track_dict, int track)

```
....
395.      snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2425
Status	New

The add_audio_for_lang method calls the snprintf function, at line 636 of HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-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	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	648	648
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method static void add_audio_for_lang(hb_value_array_t *list, const hb_dict_t *preset,

```
....
648.          snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2426
Status	New

The source_audio_track_used method calls the snprintf function, at line 387 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	391	391
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method static hb_dict_t * source_audio_track_used(hb_dict_t *track_dict, int track)

```
....
391.      snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2427
Status	New

The add_audio_for_lang method calls the snprintf function, at line 632 of HandBrake@@HandBrake-1.4.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method static void add_audio_for_lang(hb_value_array_t *list, const hb_dict_t *preset,

```
....
644.          snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 27:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2428
Status	New

The source_audio_track_used method calls the snprintf function, at line 387 of HandBrake@@HandBrake-1.5.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	391	391
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method static hb_dict_t * source_audio_track_used(hb_dict_t *track_dict, int track)

```
....
391.      snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2429
Status	New

The add_audio_for_lang method calls the snprintf function, at line 632 of HandBrake@@HandBrake-1.5.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method static void add_audio_for_lang(hb_value_array_t *list, const hb_dict_t *preset,

```
....
644.          snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2430
Status	New

The source_audio_track_used method calls the snprintf function, at line 387 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	391	391
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method static hb_dict_t * source_audio_track_used(hb_dict_t *track_dict, int track)

```
....
391.      snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2431
Status	New

The add_audio_for_lang method calls the snprintf function, at line 632 of HandBrake@@HandBrake-1.6.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method static void add_audio_for_lang(hb_value_array_t *list, const hb_dict_t *preset,

```
....
644.          snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2432
Status	New

The source_audio_track_used method calls the snprintf function, at line 387 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	391	391
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method static hb_dict_t * source_audio_track_used(hb_dict_t *track_dict, int track)

```
....
391.      snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2433
Status	New

The add_audio_for_lang method calls the snprintf function, at line 632 of HandBrake@@HandBrake-1.7.0-CVE-2023-35853-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	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	644	644
Object	snprintf	snprintf

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method static void add_audio_for_lang(hb_value_array_t *list, const hb_dict_t *preset,

```
....
644.          snprintf(key, sizeof(key), "%d", track);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2434
Status	New

The ntlm_decode_av_pair_ucs2_str method calls the out function, at line 462 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-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	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2435
Status	New

The ntlm_decode_av_pair_ucs2_str method calls the out function, at line 462 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-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	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2436
Status	New

The ntlm_decode_av_pair_ucs2_str method calls the out function, at line 462 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-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	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2437
Status	New

The ntlm_decode_av_pair_ucs2_str method calls the out function, at line 462 of gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-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	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c
Line	472	472
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-0.8.0-CVE-2023-25567-TP.c

Method	static int ntlm_decode_av_pair_ucs2_str(struct ntlm_ctx *ctx,

```
....
472.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2438
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 440 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Line	450	450
Object	out	out

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25563-TP.c
Method	static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2439
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 440 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Line	450	450
Object	out	out

Code Snippet

File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25564-FP.c
Method	static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2440
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 440 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Line	450	450
Object	out	out

Code Snippet

File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25565-FP.c
Method	static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2441
Status	New

The parse_user_name method calls the Pointer function, at line 110 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	166	166
Object	Pointer	Pointer

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method	static uint32_t parse_user_name(uint32_t *minor_status,

```
....
166.              *domain = strdup(buf);
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2442
Status	New

The parse_user_name method calls the Pointer function, at line 110 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	192	192
Object	Pointer	Pointer

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method	static uint32_t parse_user_name(uint32_t *minor_status,

```
....
192.                  *domain = strdup(at + 1);
```

Unchecked Return Value\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2443
Status	New

The parse_user_name method calls the Pointer function, at line 110 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	203	203
Object	Pointer	Pointer

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method	static uint32_t parse_user_name(uint32_t *minor_status,

```
....
203.          *username = strdup(buf);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2444
Status	New

The uid_to_name method calls the Pointer function, at line 237 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Line	247	247
Object	Pointer	Pointer

Code Snippet	
File Name	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25566-TP.c
Method	static uint32_t uid_to_name(uint32_t *minor_status, uid_t uid, char **name)

```
....
247.      *name = strdup(pw->pw_name);
```

Unchecked Return Value\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2445
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 440 of gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-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	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c	gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Line	450	450

Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.0.0-CVE-2023-25567-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
450.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2446
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 439 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-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	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Line	449	449
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25563-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2447
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 439 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-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	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c

Line	449	449
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25564-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2448
Status	New

The ntlm_decode_av_pair_u16l_str method calls the out function, at line 439 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-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	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Line	449	449
Object	out	out

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25565-TP.c
Method static int ntlm_decode_av_pair_u16l_str(struct ntlm_ctx *ctx,

```
....
449.      out = malloc(inlen * 2 + 1);
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2449
Status	New

The parse_user_name method calls the Pointer function, at line 115 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-

	25566-TP.c	25566-TP.c
Line	171	171
Object	Pointer	Pointer

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method static uint32_t parse_user_name(uint32_t *minor_status,

```
....
171.                *domain = strdup(buf);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2450
Status	New

The parse_user_name method calls the Pointer function, at line 115 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	197	197
Object	Pointer	Pointer

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method static uint32_t parse_user_name(uint32_t *minor_status,

```
....
197.                    *domain = strdup(at + 1);
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2451
Status	New

The parse_user_name method calls the Pointer function, at line 115 of gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-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	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c	gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Line	208	208
Object	Pointer	Pointer

Code Snippet
File Name gssapi@@gss-ntlmssp-v1.1.0-CVE-2023-25566-TP.c
Method static uint32_t parse_user_name(uint32_t *minor_status,

```
....
208.          *username = strdup(buf);
```

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=1000032&projectid=26&pathid=2738
Status	New

The size of the buffer used by lglob in "%s ", at line 613 of gwsw@@less-v555-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 613 of gwsw@@less-v555-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	655	655
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 2:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2739
Status	New

The size of the buffer used by lglob in "%s ", at line 613 of gwsw@@less-v555-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 613 of gwsw@@less-v555-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	655	655
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2740
Status	New

The size of the buffer used by lglob in "%s ", at line 613 of gwsw@@less-v564-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 613 of gwsw@@less-v564-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	655	655
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2741
Status	New

The size of the buffer used by lglob in "%s ", at line 613 of gwsw@@less-v564-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 613 of gwsw@@less-v564-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	655	655
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
655.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2742
Status	New

The size of the buffer used by lglob in "%s ", at line 614 of gwsw@@less-v568-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 614 of gwsw@@less-v568-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	656	656
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2743
Status	New

The size of the buffer used by lglob in "%s ", at line 614 of gwsw@@less-v568-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 614 of gwsw@@less-v568-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	656	656
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2744
Status	New

The size of the buffer used by lglob in "%s ", at line 614 of gwsw@@less-v580-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 614 of gwsw@@less-v580-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	656	656
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v580-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2745
Status	New

The size of the buffer used by lglob in "%s ", at line 614 of gwsw@@less-v580-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 614 of gwsw@@less-v580-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	656	656
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
656.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2746
Status	New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v590-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v590-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	660	660

Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2747
Status	New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v590-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v590-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2748
Status	New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v594-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v594-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination

File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v594-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2749
Status	New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v594-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v594-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2750
Status	New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v600-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source

buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v600-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2751
Status New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v600-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v600-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2752
Status New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v605-CVE-2022-48624-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v605-CVE-2022-48624-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2753
Status New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v605-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v605-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 17:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2754
Status	New

The size of the buffer used by lglob in "%s ", at line 618 of gwsw@@less-v609-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 618 of gwsw@@less-v609-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	660	660
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method lglob(filename)

```
....
660.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2755
Status	New

The size of the buffer used by lglob in "%s ", at line 595 of gwsw@@less-v624-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 595 of gwsw@@less-v624-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v624-CVE-2024-32487-TP.c	gwsw@@less-v624-CVE-2024-32487-TP.c
Line	636	636
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v624-CVE-2024-32487-TP.c
Method public char * lglob(char *filename)

```
....
636.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2756
Status	New

The size of the buffer used by lglob in "%s ", at line 595 of gwsw@@less-v634-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 595 of gwsw@@less-v634-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v634-CVE-2024-32487-TP.c	gwsw@@less-v634-CVE-2024-32487-TP.c
Line	636	636
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v634-CVE-2024-32487-TP.c
Method public char * lglob(char *filename)

```
....
636.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2757
Status	New

The size of the buffer used by lglob in "%s ", at line 595 of gwsw@@less-v644-CVE-2024-32487-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that lglob passes to "%s ", at line 595 of gwsw@@less-v644-CVE-2024-32487-TP.c, to overwrite the target buffer.

	Source	Destination
File	gwsw@@less-v644-CVE-2024-32487-TP.c	gwsw@@less-v644-CVE-2024-32487-TP.c
Line	636	636
Object	"%s "	"%s "

Code Snippet
File Name gwsw@@less-v644-CVE-2024-32487-TP.c
Method public char * lglob(char *filename)

```
....
636.                    sprintf(gfilename + strlen(gfilename), "%s ",
qfilename);
```

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=1000032&projectid=26&pathid=3022
Status	New

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	469	469
Object	data	data

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3023
Status	New

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	469	469
Object	data	data

Code Snippet	
File Name	gwsw@@less-v555-CVE-2024-32487-TP.c
Method	bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3024
Status	New

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	469	469
Object	data	data

Code Snippet	
File Name	gwsw@@less-v564-CVE-2022-48624-TP.c
Method	bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3025
Status	New

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	469	469
Object	data	data

Code Snippet	
File Name	gwsw@@less-v564-CVE-2024-32487-TP.c
Method	bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3026
Status	New

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	469	469
Object	data	data

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3027
Status	New

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	469	469
Object	data	data

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3028
Status	New

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	469	469
Object	data	data

Code Snippet
File Name gwsw@@less-v580-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3029
Status	New

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	469	469
Object	data	data

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
469.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3030
Status	New

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3031
Status New

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3032
Status New

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	474	474

Object	data	data

Code Snippet
File Name gwsw@@less-v594-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3033
Status New

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3034
Status New

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3035
Status	New

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3036
Status	New

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 16:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3037
Status	New

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3038
Status	New

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	474	474
Object	data	data

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method bin_file(f)

```
....
474.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3039
Status	New

	Source	Destination
File	gwsw@@less-v624-CVE-2024-32487-TP.c	gwsw@@less-v624-CVE-2024-32487-TP.c
Line	458	458
Object	data	data

Code Snippet
File Name gwsw@@less-v624-CVE-2024-32487-TP.c
Method public int bin_file(int f)

```
....
458.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3040
Status New

	Source	Destination
File	gwsw@@less-v634-CVE-2024-32487-TP.c	gwsw@@less-v634-CVE-2024-32487-TP.c
Line	458	458
Object	data	data

Code Snippet
File Name gwsw@@less-v634-CVE-2024-32487-TP.c
Method public int bin_file(int f)

```
....
458.        n = read(f, data, sizeof(data));
```

Improper Resource Access Authorization\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3041
Status New

	Source	Destination
File	gwsw@@less-v644-CVE-2024-32487-TP.c	gwsw@@less-v644-CVE-2024-32487-TP.c
Line	458	458

Object	data	data

Code Snippet
File Name gwsw@@less-v644-CVE-2024-32487-TP.c
Method public int bin_file(int f)

```
....
458.        n = read(f, data, sizeof(data));
```

TOCTOU

Query Path:
CPP\Cx\CPP Low Visibility\TOCTOU Version:1

Description

TOCTOU\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3042
Status	New

The dirfile method in gwsw@@less-v555-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v555-CVE-2022-48624-TP.c	gwsw@@less-v555-CVE-2022-48624-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v555-CVE-2022-48624-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3043
Status	New

The dirfile method in gwsw@@less-v555-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v555-CVE-2024-32487-TP.c	gwsw@@less-v555-CVE-2024-32487-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v555-CVE-2024-32487-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3044
Status New

The dirfile method in gwsw@@less-v564-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v564-CVE-2022-48624-TP.c	gwsw@@less-v564-CVE-2022-48624-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v564-CVE-2022-48624-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 4:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3045
Status New

The dirfile method in gwsw@@less-v564-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v564-CVE-2024-32487-TP.c	gwsw@@less-v564-CVE-2024-32487-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v564-CVE-2024-32487-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 5:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3046
Status New

The dirfile method in gwsw@@less-v568-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v568-CVE-2022-48624-TP.c	gwsw@@less-v568-CVE-2022-48624-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v568-CVE-2022-48624-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 6:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3047
Status New

The dirfile method in gwsw@@less-v568-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v568-CVE-2024-32487-TP.c	gwsw@@less-v568-CVE-2024-32487-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v568-CVE-2024-32487-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 7:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3048
Status New

The dirfile method in gwsw@@less-v580-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v580-CVE-2022-48624-TP.c	gwsw@@less-v580-CVE-2022-48624-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v580-CVE-2022-48624-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 8:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3049
Status New

The dirfile method in gwsw@@less-v580-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v580-CVE-2024-32487-TP.c	gwsw@@less-v580-CVE-2024-32487-TP.c
Line	234	234
Object	open	open

Code Snippet
File Name gwsw@@less-v580-CVE-2024-32487-TP.c
Method dirfile(dirname, filename)

```
....
234.        f = open(pathname, OPEN_READ);
```

TOCTOU\Path 9:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3050
Status New

The dirfile method in gwsw@@less-v590-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v590-CVE-2022-48624-TP.c	gwsw@@less-v590-CVE-2022-48624-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v590-CVE-2022-48624-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 10:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3051
Status New

The dirfile method in gwsw@@less-v590-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v590-CVE-2024-32487-TP.c	gwsw@@less-v590-CVE-2024-32487-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v590-CVE-2024-32487-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3052
Status New

The dirfile method in gwsw@@less-v594-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v594-CVE-2022-48624-TP.c	gwsw@@less-v594-CVE-2022-48624-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v594-CVE-2022-48624-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 12:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3053
Status New

The dirfile method in gwsw@@less-v594-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v594-CVE-2024-32487-TP.c	gwsw@@less-v594-CVE-2024-32487-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v594-CVE-2024-32487-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3054
Status New

The dirfile method in gwsw@@less-v600-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v600-CVE-2022-48624-TP.c	gwsw@@less-v600-CVE-2022-48624-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v600-CVE-2022-48624-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 14:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3055
Status New

The dirfile method in gwsw@@less-v600-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v600-CVE-2024-32487-TP.c	gwsw@@less-v600-CVE-2024-32487-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v600-CVE-2024-32487-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 15:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3056
Status New

The dirfile method in gwsw@@less-v605-CVE-2022-48624-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v605-CVE-2022-48624-TP.c	gwsw@@less-v605-CVE-2022-48624-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v605-CVE-2022-48624-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3057
Status New

The dirfile method in gwsw@@less-v605-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v605-CVE-2024-32487-TP.c	gwsw@@less-v605-CVE-2024-32487-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v605-CVE-2024-32487-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3058
Status New

The dirfile method in gwsw@@less-v609-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v609-CVE-2024-32487-TP.c	gwsw@@less-v609-CVE-2024-32487-TP.c
Line	244	244
Object	open	open

Code Snippet
File Name gwsw@@less-v609-CVE-2024-32487-TP.c
Method dirfile(dirname, filename, must_exist)

```
....
244.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 18:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3059
Status New

The dirfile method in gwsw@@less-v624-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v624-CVE-2024-32487-TP.c	gwsw@@less-v624-CVE-2024-32487-TP.c
Line	236	236
Object	open	open

Code Snippet
File Name gwsw@@less-v624-CVE-2024-32487-TP.c
Method public char * dirfile(char *dirname, char *filename, int must_exist)

```
....
236.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 19:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3060
Status New

The dirfile method in gwsw@@less-v634-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v634-CVE-2024-32487-TP.c	gwsw@@less-v634-CVE-2024-32487-TP.c
Line	236	236
Object	open	open

Code Snippet
File Name gwsw@@less-v634-CVE-2024-32487-TP.c
Method public char * dirfile(char *dirname, char *filename, int must_exist)

```
....
236.              f = open(pathname, OPEN_READ);
```

TOCTOU\Path 20:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=3061
Status New

The dirfile method in gwsw@@less-v644-CVE-2024-32487-TP.c file utilizes open that is accessed by other concurrent functionality in a way that is not thread-safe, which may result in a Race Condition over this resource.

	Source	Destination
File	gwsw@@less-v644-CVE-2024-32487-TP.c	gwsw@@less-v644-CVE-2024-32487-TP.c
Line	236	236
Object	open	open

Code Snippet
File Name gwsw@@less-v644-CVE-2024-32487-TP.c
Method public char * dirfile(char *dirname, char *filename, int must_exist)

```
....
236.              f = open(pathname, OPEN_READ);
```

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=1000032&projectid=26&pathid=2478
Status New

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-FP.c	h2o@@h2o-newest-CVE-2021-21309-FP.c
Line	1021	1021
Object	sizeof	sizeof

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1021.              vector = s_realloc(vector,((*argc)+1)*sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2479
Status New

	Source	Destination
File	h2o@@h2o-newest-CVE-2021-21309-	h2o@@h2o-newest-CVE-2021-21309-

	FP.c	FP.c
Line	1027	1027
Object	sizeof	sizeof

Code Snippet
File Name h2o@@h2o-newest-CVE-2021-21309-FP.c
Method sds *sdssplitargs(const char *line, int *argc) {

```
....
1027.               if (vector == NULL) vector = s_malloc(sizeof(void*));
```

Use of Sizeof On a Pointer Type\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2480
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	3894	3894
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
3894.       files = malloc(count * 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=1000032&projectid=26&pathid=2481
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	3926	3926
Object	sizeof	sizeof

Code Snippet

File Name	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method	int hb_presets_add_path(char * path)

```
....
3926.       qsort(files, count, sizeof(char*), compare_str);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2482
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	3905	3905
Object	sizeof	sizeof

Code Snippet

File Name	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method	int hb_presets_add_path(char * path)

```
....
3905.       files = malloc(count * 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=1000032&projectid=26&pathid=2483
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	3937	3937
Object	sizeof	sizeof

Code Snippet

File Name	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method	int hb_presets_add_path(char * path)

```
....
3937.       qsort(files, count, sizeof(char*), compare_str);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2484
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	4159	4159
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4159.       files = malloc(count * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2485
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	4191	4191
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4191.       qsort(files, count, sizeof(char*), compare_str);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2486
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	4159	4159
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4159.       files = malloc(count * 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=1000032&projectid=26&pathid=2487
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	4191	4191
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4191.       qsort(files, count, sizeof(char*), compare_str);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2488
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	4218	4218

Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4218.       files = malloc(count * 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=1000032&projectid=26&pathid=2489
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	4250	4250
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4250.       qsort(files, count, sizeof(char*), compare_str);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2490
Status New

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	4261	4261
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4261.       files = malloc(count * sizeof(char*));
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2491
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	4293	4293
Object	sizeof	sizeof

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method int hb_presets_add_path(char * path)

```
....
4293.       qsort(files, count, sizeof(char*), compare_str);
```

Arithmenic Operation On Boolean

Query Path:
CPP\Cx\CPP Low Visibility\Arithmenic Operation On Boolean Version:1

Categories

FISMA 2014: Audit And Accountability
NIST SP 800-53: SC-5 Denial of Service Protection (P1)

Description

Arithmenic Operation On Boolean\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2758
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Line	2890	2890
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	HandBrake@@HandBrake-1.3.2-CVE-2023-35853-FP.c
Method	static void import_deint_11_0_0(hb_value_t *preset)

```
....
2890.       mode = yadif + (yadif && spatial) * 2 + bob * 4;
```

Arithmenic Operation On Boolean\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2759
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Line	2899	2899
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	HandBrake@@HandBrake-1.4.0-beta.1-CVE-2023-35853-FP.c
Method	static void import_deint_11_0_0(hb_value_t *preset)

```
....
2899.       mode = yadif + (yadif && spatial) * 2 + bob * 4;
```

Arithmenic Operation On Boolean\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2760
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Line	3141	3141
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	HandBrake@@HandBrake-1.4.0-CVE-2023-35853-FP.c
Method	static void import_deint_11_0_0(hb_value_t *preset)

```
....
3141.       mode = yadif + (yadif && spatial) * 2 + bob * 4;
```

Arithmenic Operation On Boolean\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2761
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Line	3141	3141
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name HandBrake@@HandBrake-1.5.0-CVE-2023-35853-FP.c
Method static void import_deint_11_0_0(hb_value_t *preset)

```
....
3141.       mode = yadif + (yadif && spatial) * 2 + bob * 4;
```

Arithmenic Operation On Boolean\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2762
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Line	3186	3186
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name HandBrake@@HandBrake-1.6.0-CVE-2023-35853-FP.c
Method static void import_deint_11_0_0(hb_value_t *preset)

```
....
3186.       mode = yadif + (yadif && spatial) * 2 + bob * 4;
```

Arithmenic Operation On Boolean\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000032&projectid=26&pathid=2763
Status	New

	Source	Destination
File	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c	HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Line	3208	3208
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name HandBrake@@HandBrake-1.7.0-CVE-2023-35853-FP.c
Method static void import_deint_11_0_0(hb_value_t *preset)

```
....
3208.       mode = yadif + (yadif && spatial) * 2 + bob * 4;
```

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

Buffer Overflow IndexFromInput

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

Buffer Overflow boundcpy WrongSizeParam

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Wrong Size t Allocation

Risk

What might happen

Incorrect allocation of memory may result in unexpected behavior by either overwriting sections of memory with unexpected values. Under certain conditions where both an incorrect allocation of memory and the values being written can be controlled by an attacker, such an issue may result in execution of malicious code.

Cause

How does it happen

Some memory allocation functions require a size value to be provided as a parameter. The allocated size should be derived from the provided value, by providing the length value of the intended source, multiplied by the size of that length. Failure to perform the correct arithmetic to obtain the exact size of the value will likely result in the source overflowing its destination.

General Recommendations

How to avoid it

- Always perform the correct arithmetic to determine size.
- Specifically for memory allocation, calculate the allocation size from the allocation source:
  - Derive the size value from the length of intended source to determine the amount of units to be processed.
  - Always programmatically consider the size of the each unit and their conversion to memory units - for example, by using sizeof() on the unit's type.
  - Memory allocation should be a multiplication of the amount of units being written, times the size of each unit.

Source Code Examples

CPP

Allocating and Assigning Memory without Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5);
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Allocating and Assigning Memory with Sizeof Arithmetic

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
```

```
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1;
}
```

Incorrect Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc(wcslen(source) + 1); // Would not crash for a short "source"
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Correct Arithmetic of Multi-Byte String Allocation

```
wchar_t * dest;
dest = (wchar_t *)malloc((wcslen(source) + 1) * sizeof(wchar_t));
wcscpy((wchar_t *)dest, source);
wprintf(L"Dest: %s\r\n", dest);
```

Char 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;
}
```

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

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;
}
```

Double Free

Weakness ID: 415 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The product calls free() twice on the same memory address, potentially leading to modification of unexpected memory locations.

Extended Description

When a program calls free() twice with the same argument, the program's memory management data structures become corrupted. This corruption can cause the program to crash or, in some circumstances, cause two later calls to malloc() to return the same pointer. If malloc() returns the same value twice and the program later gives the attacker control over the data that is written into this doubly-allocated memory, the program becomes vulnerable to a buffer overflow attack.

Alternate Terms

Double-free

Time of Introduction

- Architecture and Design
- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Access Control	Doubly freeing memory may result in a write-what-where condition, allowing an attacker to execute arbitrary code.

Likelihood of Exploit

Low to Medium

Demonstrative Examples

Example 1

The following code shows a simple example of a double free vulnerability.

(Bad Code)

Example Language: **C**

```
char* ptr = (char*)malloc (SIZE);
...
if (abrt) {
free(ptr);
}
...
free(ptr);
```

Double free vulnerabilities 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

Although some double free vulnerabilities are not much more complicated than the previous example, most are spread out across hundreds of lines of code or even different files. Programmers seem particularly susceptible to freeing global variables

more than once.

Example 2

While contrived, this code should be exploitable on Linux distributions which do not ship with heap-chunk check summing turned on.

(Bad Code)

Example Language: **C**

```
#include <stdio.h>
#include <unistd.h>
#define BUFSIZE1 512
#define BUFSIZE2 ((BUFSIZE1/2) - 8)

int main(int argc, char **argv) {
char *buf1R1;
char *buf2R1;
char *buf1R2;
buf1R1 = (char *) malloc(BUFSIZE2);
buf2R1 = (char *) malloc(BUFSIZE2);
free(buf1R1);
free(buf2R1);
buf1R2 = (char *) malloc(BUFSIZE1);
strncpy(buf1R2, argv[1], BUFSIZE1-1);
free(buf2R1);
free(buf1R2);
}
```

Observed Examples

Reference	Description
CVE-2004-0642	Double free resultant from certain error conditions.
CVE-2004-0772	Double free resultant from certain error conditions.
CVE-2005-1689	Double free resultant from certain error conditions.
CVE-2003-0545	Double free from invalid ASN.1 encoding.
CVE-2003-1048	Double free from malformed GIF.
CVE-2005-0891	Double free from malformed GIF.
CVE-2002-0059	Double free from malformed compressed data.

Potential Mitigations

Phase: Architecture and Design

Choose a language that provides automatic memory management.

Phase: Implementation

Ensure that each allocation is freed only once. After freeing a chunk, set the pointer to NULL to ensure the pointer cannot be freed again. In complicated error conditions, be sure that clean-up routines respect the state of allocation properly. If the language is object oriented, ensure that object destructors delete each chunk of memory only once.

Phase: Implementation

Use a static analysis tool to find double free instances.

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	Weakness Base	666	Operation on Resource in Wrong Phase of	**Research Concepts (primary)1000**

			Lifetime	
ChildOf	Weakness Class	675	Duplicate Operations on Resource	Research Concepts1000
ChildOf	Category	742	CERT C Secure Coding Section 08 - Memory Management (MEM)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
PeerOf	Weakness Base	123	Write-what-where Condition	Research Concepts1000
PeerOf	Weakness Base	416	Use After Free	Development Concepts699 Research Concepts1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**
PeerOf	Weakness Base	364	Signal Handler Race Condition	Research Concepts1000

Relationship Notes

This is usually resultant from another weakness, such as an unhandled error or race condition between threads. It could also be primary to weaknesses such as buffer overflows.

Affected Resources

- Memory

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
PLOVER			DFREE - Double-Free Vulnerability
7 Pernicious Kingdoms			Double Free
CLASP			Doubly freeing memory
CERT C Secure Coding	MEM00-C		Allocate and free memory in the same module, at the same level of abstraction
CERT C Secure Coding	MEM01-C		Store a new value in pointers immediately after free()
CERT C Secure Coding	MEM31-C		Free dynamically allocated memory exactly once

White Box Definitions

A weakness where code path has:

1. start statement that relinquishes a dynamically allocated memory resource
2. end statement that relinquishes the dynamically allocated memory resource

Maintenance Notes

It could be argued that Double Free would be most appropriately located as a child of "Use after Free", but "Use" and "Release" are considered to be distinct operations within vulnerability theory, therefore this is more accurately "Release of a Resource after Expiration or Release", which doesn't exist yet.

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 Potential Mitigations, Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Maintenance Notes, Relationships, Other Notes, Relationship Notes, Taxonomy Mappings		
2008-11-24	CWE Content Team	MITRE	Internal

	updated Relationships, Taxonomy Mappings		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Other Notes		

BACK TO TOP

MemoryFree on StackVariable

Risk

What might happen

Undefined Behavior may result with a crash. Crashes may give an attacker valuable information about the system and the program internals. Furthermore, it may leave unprotected files (e.g memory) that may be exploited.

Cause

How does it happen

Calling free() on a variable that was not dynamically allocated (e.g. malloc) will result with an Undefined Behavior.

General Recommendations

How to avoid it

Use free() only on dynamically allocated variables in order to prevent unexpected behavior from the compiler.

Source Code Examples

CPP

Bad - Calling free() on a static variable

```
void clean_up(){
  char temp[256];
  do_something();
  free(tmp);
  return;
}
```

Good - Calling free() only on variables that were dynamically allocated

```
void clean_up(){
  char *buff;
  buff = (char*) malloc(1024);
  free(buff);
  return;
}
```

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 Uninitialized Variable

Weakness ID: 457 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code uses a variable that has not been initialized, leading to unpredictable or unintended results.

Extended Description

In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Sometimes)*

C++: *(Sometimes)*

Perl: *(Often)*

All

Common Consequences

Scope	Effect
Availability Integrity	Initial variables usually contain junk, which can not be trusted for consistency. This can lead to denial of service conditions, or modify control flow in unexpected ways. In some cases, an attacker can "pre-initialize" the variable using previous actions, which might enable code execution. This can cause a race condition if a lock variable check passes when it should not.
Authorization	Strings that are not initialized are especially dangerous, since many functions expect a null at the end -- and only at the end -- of a string.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

The following switch statement is intended to set the values of the variables aN and bN, but in the default case, the programmer has accidentally set the value of aN twice. As a result, bN will have an undefined value.

(Bad Code)

Example Language: **C**

```
switch (ctl) {
case -1:
aN = 0;
bN = 0;
break;
case 0:
aN = i;
bN = -i;
break;
case 1:
aN = i + NEXT_SZ;
bN = i - NEXT_SZ;
break;
default:
```

```
aN = -1;
aN = -1;
break;
}
repaint(aN, bN);
```

Most uninitialized variable issues result in general software reliability problems, but if attackers can intentionally trigger the use of an uninitialized variable, they might be able to launch a denial of service attack by crashing the program. Under the right circumstances, an attacker may be able to control the value of an uninitialized variable by affecting the values on the stack prior to the invocation of the function.

Example 2

Example Languages: **C++ and Java**

```
int foo;
void bar() {
if (foo==0)
/.../
/../
}
```

Observed Examples

Reference	Description
CVE-2008-0081	Uninitialized variable leads to code execution in popular desktop application.
CVE-2007-4682	Crafted input triggers dereference of an uninitialized object pointer.
CVE-2007-3468	Crafted audio file triggers crash when an uninitialized variable is used.
CVE-2007-2728	Uninitialized random seed variable used.

Potential Mitigations

Phase: Implementation

Assign all variables to an initial value.

Phase: Build and Compilation

Most compilers will complain about the use of uninitialized variables if warnings are turned on.

Phase: Requirements

The choice could be made to use a language that is not susceptible to these issues.

Phase: Architecture and Design

Mitigating technologies such as safe string libraries and container abstractions could be introduced.

Other Notes

Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Stack variables in C and C++ are not initialized by default. Their initial values are determined by whatever happens to be in their location on the stack at the time the function is invoked. Programs should never use the value of an uninitialized variable. It is not uncommon for programmers to use an uninitialized variable in code that handles errors or other rare and exceptional circumstances. Uninitialized variable warnings can sometimes indicate the presence of a typographic error in the code.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	398	Indicator of Poor Code Quality	**Seven Pernicious Kingdoms (primary)700**
ChildOf	Weakness Base	456	Missing Initialization	**Development Concepts (primary)699 Research Concepts**

				(primary)1000
MemberOf	View	630	Weaknesses Examined by SAMATE	**Weaknesses Examined by SAMATE (primary)630**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Uninitialized variable
7 Pernicious Kingdoms			Uninitialized Variable

White Box Definitions

A weakness where the code path has:

1. start statement that defines variable
2. end statement that accesses the variable
3. the code path does not contain a statement that assigns value to the variable

References

mercy. "Exploiting Uninitialized Data". Jan 2006. < http://www.felinemenace.org/~mercy/papers/UBehavior/UBehavior.zip>.

Microsoft Security Vulnerability Research & Defense. "MS08-014 : The Case of the Uninitialized Stack Variable Vulnerability". 2008-03-11. <http://blogs.technet.com/swi/archive/2008/03/11/the-case-of-the-uninitialized-stack-variable-vulnerability.aspx>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Description, Relationships, Observed Example, Other Notes, References, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences, Demonstrative Examples, Potential Mitigations		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		

Previous Entry Names

Change Date	Previous Entry Name
2008-04-11	Uninitialized Variable

BACK TO TOP

Use of Zero Initialized Pointer

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

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

Indicator of Poor Code Quality

Weakness ID: 398 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The code has features that do not directly introduce a weakness or vulnerability, but indicate that the product has not been carefully developed or maintained.

Extended Description

Programs are more likely to be secure when good development practices are followed. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Time of Introduction

- Architecture and Design
- Implementation

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	18	Source Code	**Development Concepts (primary)699**
ChildOf	Weakness Class	710	Coding Standards Violation	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	107	Struts: Unused Validation Form	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	110	Struts: Validator Without Form Field	**Research Concepts (primary)1000**
ParentOf	Category	399	Resource Management Errors	**Development Concepts (primary)699**
ParentOf	Weakness Base	401	Failure to Release Memory Before Removing Last Reference ('Memory Leak')	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	404	Improper Resource Shutdown or Release	Development Concepts699 **Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	415	Double Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	416	Use After Free	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Variant	457	Use of Uninitialized Variable	**Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	474	Use of Function with Inconsistent Implementations	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	475	Undefined Behavior for Input to API	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700**
ParentOf	Weakness Base	476	NULL Pointer	**Development**

			Dereference	**Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Base	477	Use of Obsolete Functions	**Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000**
ParentOf	Weakness Variant	478	Missing Default Case in Switch Statement	**Development Concepts (primary)699**
ParentOf	Weakness Variant	479	Unsafe Function Call from a Signal Handler	**Development Concepts (primary)699**
ParentOf	Weakness Variant	483	Incorrect Block Delimitation	**Development Concepts (primary)699**
ParentOf	Weakness Base	484	Omitted Break Statement in Switch	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	546	Suspicious Comment	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	547	Use of Hard-coded, Security-relevant Constants	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	561	Dead Code	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Base	562	Return of Stack Variable Address	**Development Concepts (primary)699** Research Concepts1000
ParentOf	Weakness Variant	563	Unused Variable	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Category	569	Expression Issues	**Development Concepts (primary)699**
ParentOf	Weakness Variant	585	Empty Synchronized Block	**Development Concepts (primary)699 Research Concepts (primary)1000**
ParentOf	Weakness Variant	586	Explicit Call to Finalize()	**Development Concepts (primary)699**
ParentOf	Weakness Variant	617	Reachable Assertion	**Development Concepts (primary)699**
ParentOf	Weakness Base	676	Use of Potentially Dangerous Function	**Development Concepts (primary)699 Research Concepts (primary)1000**
MemberOf	View	700	Seven Pernicious Kingdoms	**Seven Pernicious Kingdoms (primary)700**

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name

7 Pernicious Kingdoms			Code Quality

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		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Description, Relationships, Taxonomy Mappings		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Relationships		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2008-04-11	Code Quality		

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

TOCTOU

Risk

What might happen

At best, a Race Condition may cause errors in accuracy, overidden values or unexpected behavior that may result in denial-of-service. At worst, it may allow attackers to retrieve data or bypass security processes by replaying a controllable Race Condition until it plays out in their favor.

Cause

How does it happen

Race Conditions occur when a public, single instance of a resource is used by multiple concurrent logical processes. If the these logical processes attempt to retrieve and update the resource without a timely management system, such as a lock, a Race Condition will occur.

An example for when a Race Condition occurs is a resource that may return a certain value to a process for further editing, and then updated by a second process, resulting in the original process' data no longer being valid. Once the original process edits and updates the incorrect value back into the resource, the second process' update has been overwritten and lost.

General Recommendations

How to avoid it

When sharing resources between concurrent processes across the application ensure that these resources are either thread-safe, or implement a locking mechanism to ensure expected concurrent activity.

Source Code Examples

Java

Different Threads Increment and Decrement The Same Counter Repeatedly, Resulting in a Race Condition

```
      public static int counter = 0;
      public static void start() throws InterruptedException {
             incrementCounter ic;
             decrementCounter dc;
             while(counter == 0) {
                    counter = 0;
                    ic = new incrementCounter();
                    dc = new decrementCounter();
                    ic.start();
                    dc.start();
                    ic.join();
                    dc.join();
             }
             System.out.println(counter); //Will stop and return either -1 or 1 due to race
condition over counter
      }

      public static class incrementCounter extends Thread {
          public void run() {
             counter++;
          }
```

```
}

public static class decrementCounter extends Thread {
    public void run() {
       counter--;
    }
}
```

Different Threads Increment and Decrement The Same Thread-Safe Counter Repeatedly, Never Resulting in a Race Condition

```
public static int counter = 0;
public static Object lock = new Object();

public static void start() throws InterruptedException {
       incrementCounter ic;
       decrementCounter dc;
       while(counter == 0) { // because of proper locking, this condition is never false
              counter = 0;
              ic = new incrementCounter();
              dc = new decrementCounter();
              ic.start();
              dc.start();
              ic.join();
              dc.join();
       }
       System.out.println(counter); // Never reached
}

public static class incrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter++;
       }
    }
}

public static class decrementCounter extends Thread {
    public void run() {
       synchronized (lock) {
              counter--;
       }
    }
}
```

Improper Validation of Array Index

Weakness ID: 129 *(Weakness Base)* **Status:** Draft

Description

Description Summary

The product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array.

Alternate Terms

out-of-bounds array index

index-out-of-range

array index underflow

Time of Introduction

- Implementation

Applicable Platforms

Languages

C: *(Often)*

C++: *(Often)*

Language-independent

Common Consequences

Scope	Effect
Integrity Availability	Unchecked array indexing will very likely result in the corruption of relevant memory and perhaps instructions, leading to a crash, if the values are outside of the valid memory area.
Integrity	If the memory corrupted is data, rather than instructions, the system will continue to function with improper values.
Confidentiality Integrity	Unchecked array indexing can also trigger out-of-bounds read or write operations, or operations on the wrong objects; i.e., "buffer overflows" are not always the result. This may result in the exposure or modification of sensitive data.
Integrity	If the memory accessible by the attacker can be effectively controlled, it may be possible to execute arbitrary code, as with a standard buffer overflow and possibly without the use of large inputs if a precise index can be controlled.
Integrity Availability Confidentiality	A single fault could allow either an overflow (CWE-788) or underflow (CWE-786) of the array index. What happens next will depend on the type of operation being performed out of bounds, but can expose sensitive information, cause a system crash, or possibly lead to arbitrary code execution.

Likelihood of Exploit

High

Detection Methods

Automated Static Analysis

This weakness can often be detected using automated static analysis tools. Many modern tools use data flow analysis or constraint-based techniques to minimize the number of false positives.

Automated static analysis generally does not account for environmental considerations when reporting out-of-bounds memory operations. This can make it difficult for users to determine which warnings should be investigated first. For example, an analysis tool might report array index errors that originate from command line arguments in a program that is not expected to run with setuid or other special privileges.

Effectiveness: High

This is not a perfect solution, since 100% accuracy and coverage are not feasible.

Automated Dynamic Analysis

This weakness can be detected using dynamic tools and techniques that interact with the software using large test suites with many diverse inputs, such as fuzz testing (fuzzing), robustness testing, and fault injection. The software's operation may slow down, but it should not become unstable, crash, or generate incorrect results.

Black Box

Black box methods might not get the needed code coverage within limited time constraints, and a dynamic test might not produce any noticeable side effects even if it is successful.

Demonstrative Examples

Example 1

The following C/C++ example retrieves the sizes of messages for a pop3 mail server. The message sizes are retrieved from a socket that returns in a buffer the message number and the message size, the message number (num) and size (size) are extracted from the buffer and the message size is placed into an array using the message number for the array index.

(Bad Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2)
sizes[num - 1] = size;
}
...
}
```

In this example the message number retrieved from the buffer could be a value that is outside the allowable range of indices for the array and could possibly be a negative number. Without proper validation of the value to be used for the array index an array overflow could occur and could potentially lead to unauthorized access to memory addresses and system crashes. The value of the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **C**

```
/* capture the sizes of all messages */
int getsizes(int sock, int count, int *sizes) {
...
char buf[BUFFER_SIZE];
int ok;
int num, size;

// read values from socket and added to sizes array
while ((ok = gen_recv(sock, buf, sizeof(buf))) == 0)
{

// continue read from socket until buf only contains '.'
if (DOTLINE(buf))
break;
else if (sscanf(buf, "%d %d", &num, &size) == 2) {
```

```
if (num > 0 && num <= (unsigned)count)
sizes[num - 1] = size;
else
/* warn about possible attempt to induce buffer overflow */
report(stderr, "Warning: ignoring bogus data for message sizes returned by server.\n");
}
}
...
}
```

Example 2

In the code snippet below, an unchecked integer value is used to reference an object in an array.

(Bad Code)

Example Language: **Java**

```
public String getValue(int index) {
return array[index];
}
```

If index is outside of the range of the array, this may result in an ArrayIndexOutOfBounds Exception being raised.

Example 3

In the following Java example the method displayProductSummary is called from a Web service servlet to retrieve product summary information for display to the user. The servlet obtains the integer value of the product number from the user and passes it to the displayProductSummary method. The displayProductSummary method passes the integer value of the product number to the getProductSummary method which obtains the product summary from the array object containing the project summaries using the integer value of the product number as the array index.

(Bad Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);

} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
return products[index];
}
```

In this example the integer value used as the array index that is provided by the user may be outside the allowable range of indices for the array which may provide unexpected results or may comes the application to fail. The integer value used for the array index should be validated to ensure that it is within the allowable range of indices for the array as in the following code.

(Good Code)

Example Language: **Java**

```
// Method called from servlet to obtain product information
public String displayProductSummary(int index) {

String productSummary = new String("");

try {
String productSummary = getProductSummary(index);
```

```
} catch (Exception ex) {...}

return productSummary;
}

public String getProductSummary(int index) {
String productSummary = "";

if ((index >= 0) && (index < MAX_PRODUCTS)) {
productSummary = products[index];
}
else {
System.err.println("index is out of bounds");
throw new IndexOutOfBoundsException();
}

return productSummary;
}
```

An alternative in Java would be to use one of the collection objects such as ArrayList that will automatically generate an exception if an attempt is made to access an array index that is out of bounds.

(Good Code)

Example Language: **Java**

```
ArrayList productArray = new ArrayList(MAX_PRODUCTS);
...
try {
productSummary = (String) productArray.get(index);
} catch (IndexOutOfBoundsException ex) {...}
```

Observed Examples

Reference	Description
CVE-2005-0369	large ID in packet used as array index
CVE-2001-1009	negative array index as argument to POP LIST command
CVE-2003-0721	Integer signedness error leads to negative array index
CVE-2004-1189	product does not properly track a count and a maximum number, which can lead to resultant array index overflow.
CVE-2007-5756	chain: device driver for packet-capturing software allows access to an unintended IOCTL with resultant array index error.

Potential Mitigations

Phase: Architecture and Design

Strategies: Input Validation; Libraries or Frameworks

Use an input validation framework such as Struts or the OWASP ESAPI Validation API. If you use Struts, be mindful of weaknesses covered by the CWE-101 category.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

Even though client-side checks provide minimal benefits with respect to server-side security, they are still useful. First, they can support intrusion detection. If the server receives input that should have been rejected by the client, then it may be an indication of an attack. Second, client-side error-checking can provide helpful feedback to the user about the expectations for valid input. Third, there may be a reduction in server-side processing time for accidental input errors, although this is typically a small savings.

Phase: Requirements

Strategy: Language Selection

Use a language with features that can automatically mitigate or eliminate out-of-bounds indexing errors.

For example, Ada allows the programmer to constrain the values of a variable and languages such as Java and Ruby will allow the programmer to handle exceptions when an out-of-bounds index is accessed.

Phase: Implementation

Strategy: Input Validation

Assume all input is malicious. Use an "accept known good" input validation strategy (i.e., use a whitelist). Reject any input that does not strictly conform to specifications, or transform it into something that does. Use a blacklist to reject any unexpected inputs and detect potential attacks.

When accessing a user-controlled array index, use a stringent range of values that are within the target array. Make sure that you do not allow negative values to be used. That is, verify the minimum as well as the maximum of the range of acceptable values.

Phase: Implementation

Be especially careful to validate your input when you invoke code that crosses language boundaries, such as from an interpreted language to native code. This could create an unexpected interaction between the language boundaries. Ensure that you are not violating any of the expectations of the language with which you are interfacing. For example, even though Java may not be susceptible to buffer overflows, providing a large argument in a call to native code might trigger an overflow.

Weakness Ordinalities

Ordinality	Description
Resultant	The most common condition situation leading to unchecked array indexing is the use of loop index variables as buffer indexes. If the end condition for the loop is subject to a flaw, the index can grow or shrink unbounded, therefore causing a buffer overflow or underflow. Another common situation leading to this condition is the use of a function's return value, or the resulting value of a calculation directly as an index in to a buffer.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Class	20	Improper Input Validation	**Development Concepts (primary)699 Research Concepts (primary)1000**
ChildOf	Category	189	Numeric Errors	Development Concepts699
ChildOf	Category	633	Weaknesses that Affect Memory	**Resource-specific Weaknesses (primary)631**
ChildOf	Category	738	CERT C Secure Coding Section 04 - Integers (INT)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
ChildOf	Category	802	2010 Top 25 - Risky Resource Management	**Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors (primary)800**
CanPrecede	Weakness Class	119	Failure to Constrain Operations within the Bounds of a Memory Buffer	Research Concepts1000
CanPrecede	Weakness Variant	789	Uncontrolled Memory Allocation	Research Concepts1000
PeerOf	Weakness Base	124	Buffer Underwrite ('Buffer Underflow')	Research Concepts1000

Theoretical Notes

An improperly validated array index might lead directly to the always-incorrect behavior of "access of array using out-of-bounds index."

Affected Resources

- Memory

f Causal Nature

Explicit

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Unchecked array indexing
PLOVER			INDEX - Array index overflow
CERT C Secure Coding	ARR00-C		Understand how arrays work
CERT C Secure Coding	ARR30-C		Guarantee that array indices are within the valid range
CERT C Secure Coding	ARR38-C		Do not add or subtract an integer to a pointer if the resulting value does not refer to a valid array element
CERT C Secure Coding	INT32-C		Ensure that operations on signed integers do not result in overflow

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
100	Overflow Buffers	

References

[REF-11] M. Howard and D. LeBlanc. "Writing Secure Code". Chapter 5, "Array Indexing Errors" Page 144. 2nd Edition. Microsoft. 2002.

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	CLASP		Externally Mined
Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Alternate Terms, Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-01-12	CWE Content Team	MITRE	Internal
	updated Common Consequences		
2009-10-29	CWE Content Team	MITRE	Internal
	updated Description, Name, Relationships		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Observed Examples, Other Notes, Potential Mitigations, Theoretical Notes, Weakness Ordinalities		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Demonstrative Examples, Detection Factors, Likelihood of Exploit, Potential Mitigations, References, Related Attack Patterns, Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Related Attack Patterns		
Previous Entry Names			
Change Date	**Previous Entry Name**		
2009-10-29	Unchecked Array Indexing		

BACK TO TOP

Scanned Languages

Language	Hash Number	Change Date
CPP	4541647240435660	1/6/2025
Common	0105849645654507	1/6/2025