vul_files_7 Scan Report

Project Name	vul_files_7
Scan Start	Monday, January 6, 2025 6:41:41 PM
Preset	Checkmarx Default
Scan Time	01h:45m:53s
Lines Of Code Scanned	299747
Files Scanned	148
Report Creation Time	Monday, January 6, 2025 7:48:05 PM
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9
Team	CxServer
Checkmarx Version	8.7.0
Scan Type	Full
Source Origin	LocalPath
Density	2/100 (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

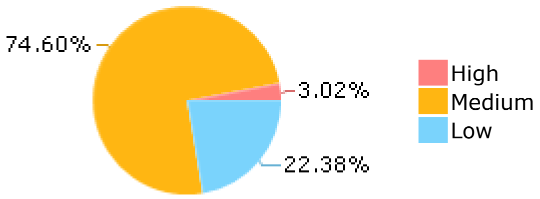
Results Limit

Results limit per query was set to 50

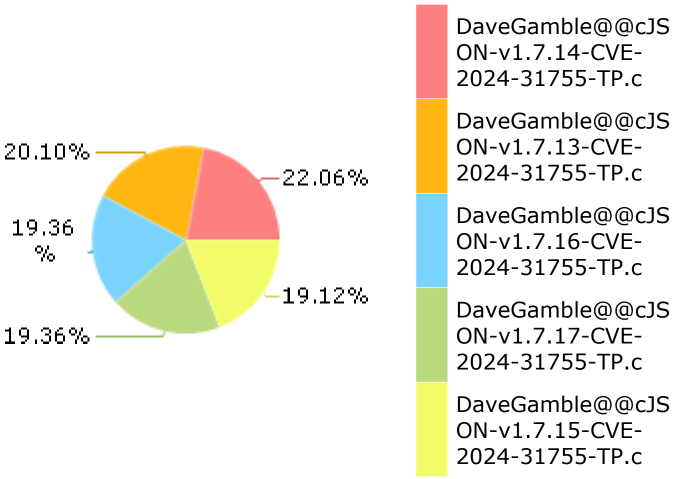
Selected Queries

Selected queries are listed in Result Summary

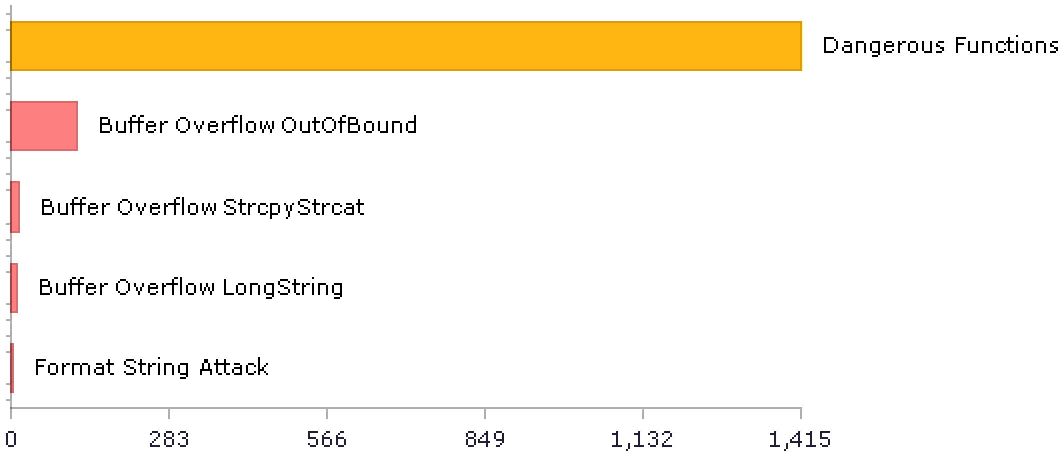
Result Summary



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	690	444
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	258	258
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	63	61
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	1415	1415
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	46	46
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	1415	1415
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	40	40
PCI DSS (3.2) - 6.5.2 - Buffer overflows	457	343
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.	62	62
Audit And Accountability*	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	9	7
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.	200	200
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.	59	59
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	22	22

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

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	263	263
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)	4	2
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)	17	17
SC-4 Information in Shared Resources (P1)	46	46
SC-5 Denial of Service Protection (P1)*	1322	855
SC-8 Transmission Confidentiality and Integrity (P1)	0	0
SI-10 Information Input Validation (P1)*	359	245
SI-11 Error Handling (P2)*	205	205
SI-15 Information Output Filtering (P0)	0	0
SI-16 Memory Protection (P1)	163	69

* 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

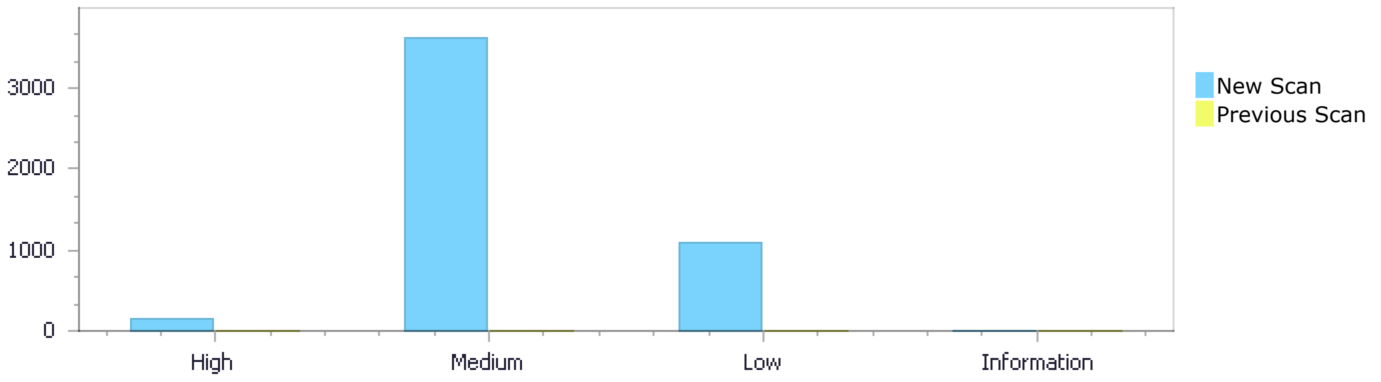
Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Results Distribution By Status

First scan of the project

	High	Medium	Low	Information	Total
New Issues	147	3,636	1,091	0	4,874
Recurrent Issues	0	0	0	0	0
Total	147	3,636	1,091	0	4,874

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	147	3,636	1,091	0	4,874
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	147	3,636	1,091	0	4,874

Result Summary

Vulnerability Type	Occurrences	Severity
Buffer Overflow OutOfBound	120	High
Buffer Overflow StrcpyStrcat	13	High
Buffer Overflow LongString	12	High
Format String Attack	2	High
Dangerous Functions	1415	Medium

Use of Zero Initialized Pointer	642	Medium
Memory Leak	468	Medium
MemoryFree on StackVariable	386	Medium
Buffer Overflow boundcpy WrongSizeParam	282	Medium
Wrong Size t Allocation	185	Medium
Double Free	123	Medium
Heap Inspection	46	Medium
Divide By Zero	32	Medium
Use of Uninitialized Variable	18	Medium
Integer Overflow	17	Medium
Wrong Memory Allocation	7	Medium
Char Overflow	6	Medium
Boolean Overflow	5	Medium
Inadequate Encryption Strength	4	Medium
Unchecked Return Value	205	Low
Improper Resource Access Authorization	196	Low
NULL Pointer Dereference	194	Low
Unchecked Array Index	150	Low
TOCTOU	85	Low
Use of Sizeof On a Pointer Type	82	Low
Incorrect Permission Assignment For Critical Resources	62	Low
Potential Off by One Error in Loops	40	Low
Sizeof Pointer Argument	28	Low
Potential Precision Problem	27	Low
Use of Insufficiently Random Values	13	Low
Exposure of System Data to Unauthorized Control Sphere	5	Low
Information Exposure Through Comments	4	Low

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c	76
curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	70
curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	70
curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	69
curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	68
curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	68
DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c	68
DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c	68
DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c	68
curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	67

Scan Results Details

Buffer Overflow OutOfBound

Query Path:
CPP\Cx\CPP Buffer Overflow\Buffer Overflow OutOfBound 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 OutOfBound\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2997
Status	New

The size of the buffer used by schannel_acquire_credential_handle in rgstrChainingModes, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	884
Object	crypto_settings	rgstrChainingModes

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
884.        crypto_settings[crypto_settings_idx].rgstrChainingModes =
```

Buffer Overflow OutOfBound\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2998
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer.

This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	882
Object	crypto_settings	eAlgorithmUsage

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
882.        crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2999
Status	New

The size of the buffer used by schannel_acquire_credential_handle in cChainingModes, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	886
Object	crypto_settings	cChainingModes

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
886.        crypto_settings[crypto_settings_idx].cChainingModes =
```

Buffer Overflow OutOfBound\Path 4:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3000
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	888
Object	crypto_settings	Length

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
888.        crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3001
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	890
Object	crypto_settings	MaximumLength

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
890.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3002
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	892
Object	crypto_settings	Buffer

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
892.        crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3003
Status	New

The size of the buffer used by schannel_acquire_credential_handle in dwMinBitLength, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c

Line	789	898
Object	crypto_settings	dwMinBitLength

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
898.            crypto_settings[crypto_settings_idx].dwMinBitLength =
128;
```

Buffer Overflow OutOfBound\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3004
Status	New

The size of the buffer used by schannel_acquire_credential_handle in dwMaxBitLength, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	900
Object	crypto_settings	dwMaxBitLength

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
900.            crypto_settings[crypto_settings_idx].dwMaxBitLength =
64;
```

Buffer Overflow OutOfBound\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3005
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	919
Object	crypto_settings	eAlgorithmUsage

Code Snippet
File Name   curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method   schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
919.          crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3006
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	927
Object	crypto_settings	Buffer

Code Snippet
File Name   curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method   schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
927.          crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 11:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3007
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	932
Object	crypto_settings	eAlgorithmUsage

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
932.          crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3008
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	934
Object	crypto_settings	Length

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
934.           crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3009
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	936
Object	crypto_settings	MaximumLength

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
936.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 14:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3010
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c

Line	789	938
Object	crypto_settings	Buffer

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
938.          crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 15:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3011
Status	New

The size of the buffer used by schannel_acquire_credential_handle in rgstrChainingModes, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	942
Object	crypto_settings	rgstrChainingModes

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
942.        crypto_settings[crypto_settings_idx].rgstrChainingModes =
```

Buffer Overflow OutOfBound\Path 16:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3012
Status	New

The size of the buffer used by schannel_acquire_credential_handle in cChainingModes, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle

passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	944
Object	crypto_settings	cChainingModes

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
944.        crypto_settings[crypto_settings_idx].cChainingModes = 1;
```

Buffer Overflow OutOfBound\Path 17:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3013
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	953
Object	crypto_settings	eAlgorithmUsage

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
953.        crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 18:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3014
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	955
Object	crypto_settings	Length

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
955.        crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 19:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3015
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	957
Object	crypto_settings	MaximumLength

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
957.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 20:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3016
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	789	959
Object	crypto_settings	Buffer

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
789.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
959.         crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 21:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3017
Status	New

The size of the buffer used by schannel_acquire_credential_handle in rgstrChainingModes, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c

Line	805	900
Object	crypto_settings	rgstrChainingModes

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
900.         crypto_settings[crypto_settings_idx].rgstrChainingModes =
```

Buffer Overflow OutOfBound\Path 22:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3018
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	898
Object	crypto_settings	eAlgorithmUsage

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
898.         crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 23:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3019
Status	New

The size of the buffer used by schannel_acquire_credential_handle in cChainingModes, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle

passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	902
Object	crypto_settings	cChainingModes

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
902.         crypto_settings[crypto_settings_idx].cChainingModes =
```

Buffer Overflow OutOfBound\Path 24:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3020
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	904
Object	crypto_settings	Length

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
904.         crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 25:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=3021
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	906
Object	crypto_settings	MaximumLength

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
906.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 26:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3022
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	908
Object	crypto_settings	Buffer

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
908.         crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 27:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3023
Status	New

The size of the buffer used by schannel_acquire_credential_handle in dwMinBitLength, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	914
Object	crypto_settings	dwMinBitLength

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
914.             crypto_settings[crypto_settings_idx].dwMinBitLength =
128;
```

Buffer Overflow OutOfBound\Path 28:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3024
Status	New

The size of the buffer used by schannel_acquire_credential_handle in dwMaxBitLength, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c

Line	805	916
Object	crypto_settings	dwMaxBitLength

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
916.            crypto_settings[crypto_settings_idx].dwMaxBitLength =
64;
```

Buffer Overflow OutOfBound\Path 29:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3025
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	935
Object	crypto_settings	eAlgorithmUsage

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
935.          crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 30:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3026
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	943
Object	crypto_settings	Buffer

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
943.          crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 31:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3027
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	948
Object	crypto_settings	eAlgorithmUsage

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
948.          crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 32:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3028
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	950
Object	crypto_settings	Length

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
950.          crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 33:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3029
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	952
Object	crypto_settings	MaximumLength

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
952.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 34:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3030
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	954
Object	crypto_settings	Buffer

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
954.            crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 35:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3031
Status	New

The size of the buffer used by schannel_acquire_credential_handle in rgstrChainingModes, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c

Line	805	958
Object	crypto_settings	rgstrChainingModes

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
958.          crypto_settings[crypto_settings_idx].rgstrChainingModes =
```

Buffer Overflow OutOfBound\Path 36:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3032
Status	New

The size of the buffer used by schannel_acquire_credential_handle in cChainingModes, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	960
Object	crypto_settings	cChainingModes

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
960.          crypto_settings[crypto_settings_idx].cChainingModes = 1;
```

Buffer Overflow OutOfBound\Path 37:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3033
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle

passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	969
Object	crypto_settings	eAlgorithmUsage

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
969.        crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 38:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3034
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	971
Object	crypto_settings	Length

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
971.        crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 39:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=3035
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	973
Object	crypto_settings	MaximumLength

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
973.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 40:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3036
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	805	975
Object	crypto_settings	Buffer

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
805.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
975.         crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 41:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3037
Status	New

The size of the buffer used by schannel_acquire_credential_handle in rgstrChainingModes, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	905
Object	crypto_settings	rgstrChainingModes

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
905.         crypto_settings[crypto_settings_idx].rgstrChainingModes =
```

Buffer Overflow OutOfBound\Path 42:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3038
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	903
Object	crypto_settings	eAlgorithmUsage

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
903.        crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 43:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3039
Status	New

The size of the buffer used by schannel_acquire_credential_handle in cChainingModes, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	907
Object	crypto_settings	cChainingModes

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
907.        crypto_settings[crypto_settings_idx].cChainingModes =
```

Buffer Overflow OutOfBound\Path 44:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3040
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Length, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-	curl@@curl-curl-8_1_0-CVE-2021-

	22890-FP.c	22890-FP.c
Line	810	909
Object	crypto_settings	Length

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
909.         crypto_settings[crypto_settings_idx].strCngAlgId.Length =
```

Buffer Overflow OutOfBound\Path 45:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3041
Status	New

The size of the buffer used by schannel_acquire_credential_handle in MaximumLength, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	911
Object	crypto_settings	MaximumLength

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.       CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
911.
crypto_settings[crypto_settings_idx].strCngAlgId.MaximumLength =
```

Buffer Overflow OutOfBound\Path 46:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3042
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	913
Object	crypto_settings	Buffer

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
913.        crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

Buffer Overflow OutOfBound\Path 47:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3043
Status	New

The size of the buffer used by schannel_acquire_credential_handle in dwMinBitLength, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	919
Object	crypto_settings	dwMinBitLength

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
919.            crypto_settings[crypto_settings_idx].dwMinBitLength =
128;
```

Buffer Overflow OutOfBound\Path 48:

Severity	High

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3044
Status	New

The size of the buffer used by schannel_acquire_credential_handle in dwMaxBitLength, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	921
Object	crypto_settings	dwMaxBitLength

Code Snippet	
File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.      CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
921.            crypto_settings[crypto_settings_idx].dwMaxBitLength =
64;
```

Buffer Overflow OutOfBound\Path 49:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3045
Status	New

The size of the buffer used by schannel_acquire_credential_handle in eAlgorithmUsage, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	940
Object	crypto_settings	eAlgorithmUsage

Code Snippet	
File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
940.            crypto_settings[crypto_settings_idx].eAlgorithmUsage =
```

Buffer Overflow OutOfBound\Path 50:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3046
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to crypto_settings, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	810	948
Object	crypto_settings	Buffer

Code Snippet	
File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
810.        CRYPTO_SETTINGS crypto_settings[4] = { 0 };
....
948.            crypto_settings[crypto_settings_idx].strCngAlgId.Buffer =
```

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=1000014&projectid=9&pathid=15
Status	New

The size of the buffer used by Curl_sec_read_msg in buffer, at line 686 of curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_sec_read_msg passes to buffer, at line 686 of curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	687	738
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
687.                           char *buffer, enum protection_level level)
....
738.    strcpy(buffer, buf);
```

Buffer Overflow StrcpyStrcat\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=16
Status	New

The size of the buffer used by multissl_version in buffer, at line 1307 of curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multissl_version passes to buffer, at line 1307 of curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	1307	1347
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	static size_t multissl_version(char *buffer, size_t size)

```
....
1307.  static size_t multissl_version(char *buffer, size_t size)
....
1347.    strcpy(buffer, backends);
```

Buffer Overflow StrcpyStrcat\Path 3:

Severity	High
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=17
Status	New

The size of the buffer used by Curl_sec_read_msg in buffer, at line 674 of curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_sec_read_msg passes to buffer, at line 674 of curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c
Line	675	726
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
675.                        char *buffer, enum protection_level level)
....
726.    strcpy(buffer, buf);
```

Buffer Overflow StrcpyStrcat\Path 4:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=18
Status	New

The size of the buffer used by multissl_version in buffer, at line 1336 of curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multissl_version passes to buffer, at line 1336 of curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	1336	1376
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method	static size_t multissl_version(char *buffer, size_t size)

```
....
1336.   static size_t multissl_version(char *buffer, size_t size)
....
1376.     strcpy(buffer, backends);
```

Buffer Overflow StrcpyStrcat\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=19
Status	New

The size of the buffer used by Curl_sec_read_msg in buffer, at line 673 of curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_sec_read_msg passes to buffer, at line 673 of curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c
Line	674	725
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
674.                          char *buffer, enum protection_level level)
....
725.    strcpy(buffer, buf);
```

Buffer Overflow StrcpyStrcat\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=20
Status	New

The size of the buffer used by multissl_version in buffer, at line 1344 of curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multissl_version passes to buffer, at line 1344 of curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	1344	1384
Object	buffer	buffer

Code Snippet	
File Name	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method	static size_t multissl_version(char *buffer, size_t size)

```
....
1344.  static size_t multissl_version(char *buffer, size_t size)
....
1384.    strcpy(buffer, backends);
```

Buffer Overflow StrcpyStrcat\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=21
Status	New

The size of the buffer used by Curl_sec_read_msg in buffer, at line 673 of curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_sec_read_msg passes to buffer, at line 673 of curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c
Line	674	725
Object	buffer	buffer

Code Snippet	
File Name	curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
674.                          char *buffer, enum protection_level level)
....
725.    strcpy(buffer, buf);
```

Buffer Overflow StrcpyStrcat\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=22
Status	New

The size of the buffer used by Curl_sec_read_msg in buffer, at line 667 of curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_sec_read_msg passes to buffer, at line 667 of curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-	curl@@curl-curl-7_83_0-CVE-2022-

	32208-TP.c	32208-TP.c
Line	668	719
Object	buffer	buffer

Code Snippet

File Name curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c

Method int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
668.                           char *buffer, enum protection_level level)
....
719.    strcpy(buffer, buf);
```

Buffer Overflow StrcpyStrcat\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=23
Status	New

The size of the buffer used by print_string_ptr in output, at line 896 of DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_string_ptr passes to input, at line 896 of DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c
Line	896	918
Object	input	output

Code Snippet

File Name DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c

Method static cJSON_bool print_string_ptr(const unsigned char * const input, printbuffer * const output_buffer)

```
....
896.  static cJSON_bool print_string_ptr(const unsigned char * const
input, printbuffer * const output_buffer)
....
918.          strcpy((char*)output, "\"\"");
```

Buffer Overflow StrcpyStrcat\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=24
Status	New

The size of the buffer used by print_string_ptr in output, at line 896 of DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_string_ptr passes to input, at line 896 of DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c
Line	896	918
Object	input	output

Code Snippet

File Name	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c
Method	static cJSON_bool print_string_ptr(const unsigned char * const input, printbuffer * const output_buffer)

```
....
896.  static cJSON_bool print_string_ptr(const unsigned char * const
input, printbuffer * const output_buffer)
....
918.          strcpy((char*)output, "\"\"");
```

Buffer Overflow StrcpyStrcat\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=25
Status	New

The size of the buffer used by print_string_ptr in output, at line 898 of DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_string_ptr passes to input, at line 898 of DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c
Line	898	920
Object	input	output

Code Snippet

File Name	DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c
Method	static cJSON_bool print_string_ptr(const unsigned char * const input, printbuffer * const output_buffer)

```
....
898.  static cJSON_bool print_string_ptr(const unsigned char * const
input, printbuffer * const output_buffer)
....
920.          strcpy((char*)output, "\"\"");
```

Buffer Overflow StrcpyStrcat\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=26
Status	New

The size of the buffer used by print_string_ptr in output, at line 902 of DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_string_ptr passes to input, at line 902 of DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c
Line	902	924
Object	input	output

Code Snippet
File Name DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c
Method static cJSON_bool print_string_ptr(const unsigned char * const input, printbuffer * const output_buffer)

```
....
902.  static cJSON_bool print_string_ptr(const unsigned char * const 
input, printbuffer * const output_buffer)
....
924.            strcpy((char*)output, "\"\"");
```

Buffer Overflow StrcpyStrcat\Path 13:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=27
Status	New

The size of the buffer used by print_string_ptr in output, at line 907 of DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that print_string_ptr passes to input, at line 907 of DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c
Line	907	929
Object	input	output

Code Snippet
File Name DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c

Method static cJSON_bool print_string_ptr(const unsigned char * const input, printbuffer * const output_buffer)

```
....
907.  static cJSON_bool print_string_ptr(const unsigned char * const
input, printbuffer * const output_buffer)
....
929.          strcpy((char*)output, "\"\"");
```

Buffer Overflow LongString

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

Categories

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

Description

Buffer Overflow LongString\Path 1:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeCCM", at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	880	880
Object	"ChainingModeCCM"	Buffer

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
880.        blocked_ccm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_CCM;
```

Buffer Overflow LongString\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeGCM", at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	914	914
Object	"ChainingModeGCM"	Buffer

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
914.         blocked_gcm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_GCM;
```

Buffer Overflow LongString\Path 3:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeCCM", at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	896	896
Object	"ChainingModeCCM"	Buffer

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
896.         blocked_ccm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_CCM;
```

Buffer Overflow LongString\Path 4:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeGCM", at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	930	930
Object	"ChainingModeGCM"	Buffer

Code Snippet

File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c

Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
930.        blocked_gcm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_GCM;
```

Buffer Overflow LongString\Path 5:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=5
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeCCM", at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	901	901
Object	"ChainingModeCCM"	Buffer

Code Snippet

File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c

Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
901.        blocked_ccm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_CCM;
```

Buffer Overflow LongString\Path 6:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=6
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeGCM", at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	935	935
Object	"ChainingModeGCM"	Buffer

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
935.        blocked_gcm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_GCM;
```

Buffer Overflow LongString\Path 7:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=7
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 484 of curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeCCM", at line 484 of curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	904	904
Object	"ChainingModeCCM"	Buffer

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
904.        blocked_ccm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_CCM;
```

Buffer Overflow LongString\Path 8:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=8
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 484 of curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeGCM", at line 484 of curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	938	938
Object	"ChainingModeGCM"	Buffer

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
938.        blocked_gcm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_GCM;
```

Buffer Overflow LongString\Path 9:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=9
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 449 of curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeCCM", at line 449 of curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	866	866
Object	"ChainingModeCCM"	Buffer

Code Snippet

File Name	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
866.        blocked_ccm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_CCM;
```

Buffer Overflow LongString\Path 10:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=10
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 449 of curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeGCM", at line 449 of curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	900	900
Object	"ChainingModeGCM"	Buffer

Code Snippet

File Name	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
900.        blocked_gcm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_GCM;
```

Buffer Overflow LongString\Path 11:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=11
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 449 of curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeCCM", at line 449 of curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c

Line	866	866
Object	"ChainingModeCCM"	Buffer

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
866.        blocked_ccm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_CCM;
```

Buffer Overflow LongString\Path 12:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=12
Status	New

The size of the buffer used by schannel_acquire_credential_handle in Buffer, at line 449 of curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that schannel_acquire_credential_handle passes to "ChainingModeGCM", at line 449 of curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Line	900	900
Object	"ChainingModeGCM"	Buffer

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
900.        blocked_gcm_modes[0].Buffer = (PWSTR)BCRYPT_CHAIN_MODE_GCM;
```

Format String Attack

Query Path:
CPP\Cx\CPP Buffer Overflow\Format String Attack 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

Format String Attack\Path 1:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=13
Status	New

Method check_telnet_options at line 773 of curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c receives the "%127[^=]%*[=]%255s" value from user input. This value is then used to construct a "format string" "%127[^=]%*[=]%255s", which is provided as an argument to a string formatting function in check_telnet_options method of curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c at line 773.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	799	799
Object	"%127[^=]%*[=]%255s"	"%127[^=]%*[=]%255s"

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
799.        if(sscanf(head->data, "%127[^= ]%*[ =]%255s",
```

Format String Attack\Path 2:

Severity	High
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=14
Status	New

Method check_telnet_options at line 773 of curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c receives the "%hu%*[xX]%hu" value from user input. This value is then used to construct a "format string" "%hu%*[xX]%hu", which is provided as an argument to a string formatting function in check_telnet_options method of curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c at line 773.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	832	832
Object	"%hu%*[xX]%hu"	"%hu%*[xX]%hu"

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
832.            if(sscanf(option_arg, "%hu%*[xX]%hu",
```

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=1000014&projectid=9&pathid=555
Status	New

The dangerous function, _tcslen, was found in use at line 362 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	404	404
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
404.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=556
Status	New

The dangerous function, _tcslen, was found in use at line 362 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	404	404
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c

Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
404.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=557
Status	New

The dangerous function, _tcslen, was found in use at line 362 in curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	404	404
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
404.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=558
Status	New

The dangerous function, _tcslen, was found in use at line 362 in curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	404	404
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
404.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=559
Status	New

The dangerous function, _tcslen, was found in use at line 360 in curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	402	402
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
402.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=560
Status	New

The dangerous function, _tcslen, was found in use at line 360 in curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	402	402
Object	_tcslen	_tcslen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
402.     if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=561
Status	New

The dangerous function, _tcslen, was found in use at line 362 in curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	404	404
Object	_tcslen	_tcslen

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
404.     if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=562
Status	New

The dangerous function, _tcslen, was found in use at line 426 in curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	468	468
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
468.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=563
Status	New

The dangerous function, _tcslen, was found in use at line 425 in curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	467	467
Object	_tcslen	_tcslen

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
467.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=564
Status	New

The dangerous function, _tcslen, was found in use at line 430 in curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	472	472

Object	_tcslen	_tcslen

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
472.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=565
Status	New

The dangerous function, _tcslen, was found in use at line 429 in curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	471	471
Object	_tcslen	_tcslen

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
471.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=566
Status	New

The dangerous function, _tcslen, was found in use at line 388 in curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c

Line	430	430
Object	_tcslen	_tcslen

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
430.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=567
Status	New

The dangerous function, _tcslen, was found in use at line 388 in curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Line	430	430
Object	_tcslen	_tcslen

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
430.    if(_tcslen(*thumbprint) != CERT_THUMBPRINT_STR_LEN)
```

Dangerous Functions\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=568
Status	New

The dangerous function, memcpy, was found in use at line 59 in curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-	curl@@curl-curl-7_75_0-CVE-2022-

	32208-TP.c	32208-TP.c
Line	79	79
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method static CURLcode ftpsend(struct Curl_easy *data, struct connectdata *conn,

```
....
79.     memcpy(&s, cmd, write_len);
```

Dangerous Functions\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=569
Status	New

The dangerous function, memcpy, was found in use at line 173 in curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	199	199
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method krb5_encode(void *app_data, const void *from, int length, int level, void **to)

```
....
199.     memcpy(*to, enc.value, enc.length);
```

Dangerous Functions\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=570
Status	New

The dangerous function, memcpy, was found in use at line 549 in curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination

File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	553	553
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method buffer_read(struct krb5buffer *buf, void *data, size_t len)

```
....
553.     memcpy(data, (char *)buf->data + buf->index, len);
```

Dangerous Functions\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=571
Status	New

The dangerous function, memcpy, was found in use at line 438 in curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	766	766
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
766.           memcpy(co->path, path, pathlen);
```

Dangerous Functions\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=572
Status	New

The dangerous function, memcpy, was found in use at line 868 in curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Line	931	931
Object	memcpy	memcpy

Code Snippet
File Name   curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Method   CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
931.        memcpy(hostname, host_begin, host_end - host_begin);
```

Dangerous Functions\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=573
Status	New

The dangerous function, memcpy, was found in use at line 868 in curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Line	969	969
Object	memcpy	memcpy

Code Snippet
File Name   curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Method   CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
969.          memcpy(address, addr_begin, alen);
```

Dangerous Functions\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=574
Status	New

The dangerous function, memcpy, was found in use at line 418 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	877	877
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
877.          memcpy(&alpn_buffer[cur], ALPN_H2, ALPN_H2_LENGTH);
```

Dangerous Functions\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=575
Status	New

The dangerous function, memcpy, was found in use at line 418 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	884	884
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
884.        memcpy(&alpn_buffer[cur], ALPN_HTTP_1_1,
ALPN_HTTP_1_1_LENGTH);
```

Dangerous Functions\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=576
Status	New

The dangerous function, memcpy, was found in use at line 1001 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1120	1120
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1120.       memcpy(inbuf[0].pvBuffer, BACKEND->encdata_buffer,
```

Dangerous Functions\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=577
Status	New

The dangerous function, memcpy, was found in use at line 1610 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1661	1661
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1661.     memcpy(outbuf[1].pvBuffer, buf, len);
```

Dangerous Functions\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=578
Status	New

The dangerous function, memcpy, was found in use at line 1753 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1915	1915
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1915.            memcpy(BACKEND->decdata_buffer + BACKEND-
>decdata_offset,
```

Dangerous Functions\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=579
Status	New

The dangerous function, memcpy, was found in use at line 1753 in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	2051	2051
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
2051.      memcpy(buf, BACKEND->decdata_buffer, size);
```

Dangerous Functions\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=580
Status	New

The dangerous function, memcpy, was found in use at line 418 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	877	877
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
877.         memcpy(&alpn_buffer[cur], ALPN_H2, ALPN_H2_LENGTH);
```

Dangerous Functions\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=581
Status	New

The dangerous function, memcpy, was found in use at line 418 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	884	884
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
884.       memcpy(&alpn_buffer[cur], ALPN_HTTP_1_1,
ALPN_HTTP_1_1_LENGTH);
```

Dangerous Functions\Path 28:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=582
Status	New

The dangerous function, memcpy, was found in use at line 1001 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1120	1120
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1120.       memcpy(inbuf[0].pvBuffer, BACKEND->encdata_buffer,
```

Dangerous Functions\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=583
Status	New

The dangerous function, memcpy, was found in use at line 1610 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1661	1661
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_send(struct Curl_easy *data, int sockindex,

```
....
1661.     memcpy(outbuf[1].pvBuffer, buf, len);
```

Dangerous Functions\Path 30:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=584
Status	New

The dangerous function, memcpy, was found in use at line 1753 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1915	1915
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1915.            memcpy(BACKEND->decdata_buffer + BACKEND-
>decdata_offset,
```

Dangerous Functions\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=585
Status	New

The dangerous function, memcpy, was found in use at line 1753 in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	2051	2051
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
2051.      memcpy(buf, BACKEND->decdata_buffer, size);
```

Dangerous Functions\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=586
Status	New

The dangerous function, memcpy, was found in use at line 94 in curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	110	110
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	static CURLcode blobdup(struct curl_blob **dest,

```
....
110.      memcpy(d->data, src->data, src->len);
```

Dangerous Functions\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=587
Status	New

The dangerous function, memcpy, was found in use at line 779 in curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	800	800
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
800.    memcpy(&output[labellen + 1], value, valuelen);
```

Dangerous Functions\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=588
Status	New

The dangerous function, memcpy, was found in use at line 899 in curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	952	952
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
952.      memcpy(pinkeycopy, pinnedpubkey, pinkeylen);
```

Dangerous Functions\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=589
Status	New

The dangerous function, memcpy, was found in use at line 146 in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	168	168
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_connect(struct Curl_easy *data)

```
....
168.     memcpy(&packet[client_id_offset], client_id, MQTT_CLIENTID_LEN);
```

Dangerous Functions\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=590
Status	New

The dangerous function, memcpy, was found in use at line 247 in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	276	276
Object	memcpy	memcpy

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c

Method static CURLcode mqtt_subscribe(struct Curl_easy *data)

```
....
276.     memcpy(&packet[1], encodedsize, n);
```

Dangerous Functions\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=591
Status	New

The dangerous function, memcpy, was found in use at line 247 in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	281	281
Object	memcpy	memcpy

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c

Method static CURLcode mqtt_subscribe(struct Curl_easy *data)

```
....
281.    memcpy(&packet[5 + n], topic, topiclen);
```

Dangerous Functions\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=592
Status	New

The dangerous function, memcpy, was found in use at line 326 in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	363	363
Object	memcpy	memcpy

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c

Method static CURLcode mqtt_publish(struct Curl_easy *data)

```
....
363.    memcpy(&pkt[i], encodedbytes, encodelen);
```

Dangerous Functions\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=593
Status	New

The dangerous function, memcpy, was found in use at line 326 in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	367	367
Object	memcpy	memcpy

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_publish(struct Curl_easy *data)

```
....
367.     memcpy(&pkt[i], topic, topiclen);
```

Dangerous Functions\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=594
Status	New

The dangerous function, memcpy, was found in use at line 326 in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	369	369
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_publish(struct Curl_easy *data)

```
....
369.     memcpy(&pkt[i], payload, payloadlen);
```

Dangerous Functions\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=595
Status	New

The dangerous function, memcpy, was found in use at line 621 in curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Line	657	657
Object	memcpy	memcpy

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Method	static CURLcode pop3_state_servergreet_resp(struct Curl_easy *data,

```
....
657.            memcpy(pop3c->apoptimestamp, line + i, timestamplen);
```

Dangerous Functions\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=596
Status	New

The dangerous function, memcpy, was found in use at line 621 in curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c
Line	657	657
Object	memcpy	memcpy

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c
Method	static CURLcode pop3_state_servergreet_resp(struct Curl_easy *data,

```
....
657.            memcpy(pop3c->apoptimestamp, line + i, timestamplen);
```

Dangerous Functions\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=597
Status	New

The dangerous function, memcpy, was found in use at line 2732 in curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2810	2810
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2810.         memcpy(ubuf, login, ulen);
```

Dangerous Functions\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=598
Status	New

The dangerous function, memcpy, was found in use at line 2732 in curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2818	2818
Object	memcpy	memcpy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2818.         memcpy(pbuf, psep + 1, plen);
```

Dangerous Functions\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=599
Status	New

The dangerous function, memcpy, was found in use at line 2732 in curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2826	2826

Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2826.         memcpy(obuf, osep + 1, olen);
```

Dangerous Functions\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=600
Status	New

The dangerous function, memcpy, was found in use at line 130 in curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Line	139	139
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Method static size_t trailers_read(char *buffer, size_t size, size_t nitems,

```
....
139.      memcpy(buffer,
```

Dangerous Functions\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=601
Status	New

The dangerous function, memcpy, was found in use at line 159 in curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c

Line	330	330
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Method CURLcode Curl_fillreadbuffer(struct Curl_easy *data, size_t bytes,

```
....
330.        memcpy(data->req.upload_fromhere, hexbuffer, hexlen);
```

Dangerous Functions\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=602
Status	New

The dangerous function, memcpy, was found in use at line 159 in curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Line	343	343
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Method CURLcode Curl_fillreadbuffer(struct Curl_easy *data, size_t bytes,

```
....
343.          memcpy(data->req.upload_fromhere + nread,
```

Dangerous Functions\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=603
Status	New

The dangerous function, memcpy, was found in use at line 245 in curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-	curl@@curl-curl-7_77_0-CVE-2022-

	27776-TP.c	27776-TP.c
Line	286	286
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method char *Curl_copy_header_value(const char *header)

```
....
286.     memcpy(value, start, len);
```

Dangerous Functions\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=604
Status	New

The dangerous function, memcpy, was found in use at line 1163 in curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	1185	1185
Object	memcpy	memcpy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method static size_t readmoredata(char *buffer,

```
....
1185.       memcpy(buffer, http->postdata, (size_t)http->postsize);
```

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=1000014&projectid=9&

	pathid=3230
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by lastc at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	1071
Object	tok_buf	lastc

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
790.       char *tok_buf = NULL;
....
1071.       lastc = clist;
```

Use of Zero Initialized Pointer\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3231
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by lastc at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	1065
Object	tok_buf	lastc

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
790.       char *tok_buf = NULL;
....
1065.             lastc = clist;
```

Use of Zero Initialized Pointer\Path 3:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3232
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by cookies at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 349.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	365
Object	tok_buf	cookies

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
790.       char *tok_buf = NULL;
```

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	void Curl_cookie_loadfiles(struct Curl_easy *data)

```
....
365.           data->cookies = newcookies;
```

Use of Zero Initialized Pointer\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3233
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by cookies at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 389.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	397
Object	tok_buf	cookies

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
790.      char *tok_buf = NULL;
```

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	static void remove_expired(struct CookieInfo *cookies)

```
....
397.      co = cookies->cookies[i];
```

Use of Zero Initialized Pointer\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3234
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by cookies at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	976
Object	tok_buf	cookies

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
790.      char *tok_buf = NULL;
....
976.    clist = c->cookies[myhash];
```

Use of Zero Initialized Pointer\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3235
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by cookies at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438.

	Source	Destination

File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	1087
Object	tok_buf	cookies

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
790.        char *tok_buf = NULL;
....
1087.           c->cookies[myhash] = co;
```

Use of Zero Initialized Pointer\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3236
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 438 is not initialized when it is used by first at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 246.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	790	255
Object	tok_buf	first

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
790.        char *tok_buf = NULL;
```

File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method static const char *get_top_domain(const char * const domain, size_t *outlen)

```
....
255.          first = memrchr(domain, '.', (last - domain));
```

Use of Zero Initialized Pointer\Path 8:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3237
Status	New

The variable declared in mainco at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 1280 is not initialized when it is used by mainco at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 1280.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1286	1326
Object	mainco	mainco

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1286.     struct Cookie *mainco = NULL;
....
1326.               mainco = newco;
```

Use of Zero Initialized Pointer\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3238
Status	New

The variable declared in mainco at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 1280 is not initialized when it is used by mainco at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 1280.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1286	1360
Object	mainco	mainco

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1286.     struct Cookie *mainco = NULL;
....
1360.       mainco = array[0]; /* start here */
```

Use of Zero Initialized Pointer\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3239
Status	New

The variable declared in list at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 1609 is not initialized when it is used by list at curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c in line 1609.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1611	1636
Object	list	list

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method static struct curl_slist *cookie_list(struct Curl_easy *data)

```
....
1611.     struct curl_slist *list = NULL;
....
1636.         list = beg;
```

Use of Zero Initialized Pointer\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3240
Status	New

The variable declared in old_cred at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418 is not initialized when it is used by cred at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	433	512
Object	old_cred	cred

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
433.    struct Curl_schannel_cred *old_cred = NULL;
....
512.                    BACKEND->cred->refcount));
```

Use of Zero Initialized Pointer\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3241
Status	New

The variable declared in cert_store_path at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418 is not initialized when it is used by cert_store at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	609	743
Object	cert_store_path	cert_store

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
609.        TCHAR *cert_store_path = NULL;
....
743.          cert_store =
```

Use of Zero Initialized Pointer\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3242
Status	New

The variable declared in certdata at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418 is not initialized when it is used by certdata at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	615	691
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
615.        void *certdata = NULL;
....
691.          datablob.pbData = (BYTE*)certdata;
```

Use of Zero Initialized Pointer\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3243
Status	New

The variable declared in pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 2274 is not initialized when it is used by pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 2274.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	2279	2313
Object	pCertContextServer	pCertContextServer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
2279.     CERT_CONTEXT *pCertContextServer = NULL;
....
2313.       x509_der_len = pCertContextServer->cbCertEncoded;
```

Use of Zero Initialized Pointer\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3244
Status	New

The variable declared in pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 2274 is not initialized when it is used by pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 2274.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	2279	2312
Object	pCertContextServer	pCertContextServer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
2279.     CERT_CONTEXT *pCertContextServer = NULL;
....
2312.       x509_der = (const char *)pCertContextServer->pbCertEncoded;
```

Use of Zero Initialized Pointer\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3245
Status	New

The variable declared in old_cred at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418 is not initialized when it is used by cred at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	433	512
Object	old_cred	cred

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
433.     struct Curl_schannel_cred *old_cred = NULL;
....
512.                      BACKEND->cred->refcount));
```

Use of Zero Initialized Pointer\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3246
Status	New

The variable declared in cert_store_path at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418 is not initialized when it is used by cert_store at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c

Line	609	743
Object	cert_store_path	cert_store

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
609.        TCHAR *cert_store_path = NULL;
....
743.          cert_store =
```

Use of Zero Initialized Pointer\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3247
Status	New

The variable declared in certdata at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418 is not initialized when it is used by certdata at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	615	691
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
615.        void *certdata = NULL;
....
691.          datablob.pbData = (BYTE*)certdata;
```

Use of Zero Initialized Pointer\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3248
Status	New

The variable declared in pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 2274 is not initialized when it is used by pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 2274.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	2279	2313
Object	pCertContextServer	pCertContextServer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
2279.     CERT_CONTEXT *pCertContextServer = NULL;
....
2313.       x509_der_len = pCertContextServer->cbCertEncoded;
```

Use of Zero Initialized Pointer\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3249
Status	New

The variable declared in pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 2274 is not initialized when it is used by pCertContextServer at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 2274.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	2279	2312
Object	pCertContextServer	pCertContextServer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
2279.     CERT_CONTEXT *pCertContextServer = NULL;
....
2312.       x509_der = (const char *)pCertContextServer->pbCertEncoded;
```

Use of Zero Initialized Pointer\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3250
Status	New

The variable declared in topic at curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c in line 326 is not initialized when it is used by pkt at curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c in line 326.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	331	371
Object	topic	pkt

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method	static CURLcode mqtt_publish(struct Curl_easy *data)

```
....
331.     char *topic = NULL;
....
371.     result = mqtt_send(data, (char *)pkt, i);
```

Use of Zero Initialized Pointer\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3251
Status	New

The variable declared in ace_hostname at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 1554 is not initialized when it is used by ace_hostname at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 1554.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	1571	1587
Object	ace_hostname	ace_hostname

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_idnconvert_hostname(struct Curl_easy *data,

```
....
1571.        char *ace_hostname = NULL;
....
1587.          host->encalloc = (char *)ace_hostname;
```

Use of Zero Initialized Pointer\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3252

Status	New

The variable declared in psep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732 is not initialized when it is used by psep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2758	2818
Object	psep	psep

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2758.        psep = NULL;
....
2818.        memcpy(pbuf, psep + 1, plen);
```

Use of Zero Initialized Pointer\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3253
Status	New

The variable declared in psep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732 is not initialized when it is used by psep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2740	2818
Object	psep	psep

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2740.    const char *psep = NULL;
....
2818.        memcpy(pbuf, psep + 1, plen);
```

Use of Zero Initialized Pointer\Path 25:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3254
Status	New

The variable declared in osep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732 is not initialized when it is used by osep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2767	2826
Object	osep	osep

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2767.        osep = NULL;
....
2826.        memcpy(obuf, osep + 1, olen);
```

Use of Zero Initialized Pointer\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3255
Status	New

The variable declared in osep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732 is not initialized when it is used by osep at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2741	2826
Object	osep	osep

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2741.    const char *osep = NULL;
....
2826.        memcpy(obuf, osep + 1, olen);
```

Use of Zero Initialized Pointer\Path 27:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3256
Status	New

The variable declared in conn_temp at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by dns_entry at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3395
Object	conn_temp	dns_entry

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode resolve_server(struct Curl_easy *data,

```
....
3395.      DEBUGASSERT(conn->dns_entry == NULL);
```

Use of Zero Initialized Pointer\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3257
Status	New

The variable declared in endp at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 2989 is not initialized when it is used by dns_entry at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3055	3395
Object	endp	dns_entry

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3055.       char *endp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode resolve_server(struct Curl_easy *data,

```
....
3395.       DEBUGASSERT(conn->dns_entry == NULL);
```

Use of Zero Initialized Pointer\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3258
Status	New

The variable declared in hostaddr at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281 is not initialized when it is used by dns_entry at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3329	3396
Object	hostaddr	dns_entry

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode resolve_server(struct Curl_easy *data,

```
....
3329.             hostaddr = NULL;
....
3396.       conn->dns_entry = hostaddr;
```

Use of Zero Initialized Pointer\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3259
Status	New

The variable declared in hostaddr at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281 is not initialized when it is used by dns_entry at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281.

	Source	Destination

File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3302	3396
Object	hostaddr	dns_entry

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3302.       struct Curl_dns_entry *hostaddr = NULL;
....
3396.       conn->dns_entry = hostaddr;
```

Use of Zero Initialized Pointer\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3260
Status	New

The variable declared in conn_temp at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3281.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3351
Object	conn_temp	hostname_resolve

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3351.         conn->hostname_resolve = strdup(connhost->name);
```

Use of Zero Initialized Pointer\Path 32:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3261
Status	New

The variable declared in bundle at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 183 is not initialized when it is used by bundle at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 232.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Line	188	241
Object	bundle	bundle

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c

Method Curl_conncache_find_bundle(struct Curl_easy *data,

```
....
188.      struct connectbundle *bundle = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c

Method CURLcode Curl_conncache_add_conn(struct Curl_easy *data)

```
....
241.      bundle = Curl_conncache_find_bundle(data, conn, data-
>state.conn_cache,
```

Use of Zero Initialized Pointer\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3262
Status	New

The variable declared in conn_candidate at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 481 is not initialized when it is used by conn_candidate at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 399.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Line	490	413
Object	conn_candidate	conn_candidate

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c

Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
490.    struct connectdata *conn_candidate = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c

Method bool Curl_conncache_return_conn(struct Curl_easy *data,

```
....
413.      conn_candidate = Curl_conncache_extract_oldest(data);
```

Use of Zero Initialized Pointer\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3263
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by lastc at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	1117
Object	tok_buf	lastc

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....
824.      char *tok_buf = NULL;
....
1117.      lastc = clist;
```

Use of Zero Initialized Pointer\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3264
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by lastc at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448.

	Source	Destination

File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	1111
Object	tok_buf	lastc

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
824.      char *tok_buf = NULL;
....
1111.             lastc = clist;
```

Use of Zero Initialized Pointer\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3265
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by cookies at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 354.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	371
Object	tok_buf	cookies

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
824.      char *tok_buf = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method void Curl_cookie_loadfiles(struct Curl_easy *data)

```
....
371.         data->cookies = newcookies;
```

Use of Zero Initialized Pointer\Path 37:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3266
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by cookies at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 402.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	410
Object	tok_buf	cookies

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
824.      char *tok_buf = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	static void remove_expired(struct CookieInfo *cookies)

```
....
410.      co = cookies->cookies[i];
```

Use of Zero Initialized Pointer\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3267
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by cookies at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	1020
Object	tok_buf	cookies

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
824.       char *tok_buf = NULL;
....
1020.     clist = c->cookies[myhash];
```

Use of Zero Initialized Pointer\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3268
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by cookies at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	1133
Object	tok_buf	cookies

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
824.       char *tok_buf = NULL;
....
1133.          c->cookies[myhash] = co;
```

Use of Zero Initialized Pointer\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3269
Status	New

The variable declared in tok_buf at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 448 is not initialized when it is used by first at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 252.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	824	261
Object	tok_buf	first

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
824.        char *tok_buf = NULL;
```

▼

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	static const char *get_top_domain(const char * const domain, size_t *outlen)

```
....
261.          first = memrchr(domain, '.', (last - domain));
```

Use of Zero Initialized Pointer\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3270
Status	New

The variable declared in mainco at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 1340 is not initialized when it is used by mainco at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 1340.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1346	1392
Object	mainco	mainco

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1346.    struct Cookie *mainco = NULL;
....
1392.              mainco = newco;
```

Use of Zero Initialized Pointer\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3271
Status	New

The variable declared in mainco at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 1340 is not initialized when it is used by mainco at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 1340.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1346	1428
Object	mainco	mainco

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1346.     struct Cookie *mainco = NULL;
....
1428.       mainco = array[0]; /* start here */
```

Use of Zero Initialized Pointer\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3272
Status	New

The variable declared in list at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 1678 is not initialized when it is used by list at curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c in line 1678.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1680	1704
Object	list	list

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static struct curl_slist *cookie_list(struct Curl_easy *data)

```
....
1680.     struct curl_slist *list = NULL;
....
1704.         list = beg;
```

Use of Zero Initialized Pointer\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3273
Status	New

The variable declared in ace_hostname at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 1554 is not initialized when it is used by ace_hostname at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 1554.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	1571	1587
Object	ace_hostname	ace_hostname

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_idnconvert_hostname(struct Curl_easy *data,

```
....
1571.         char *ace_hostname = NULL;
....
1587.           host->encalloc = (char *)ace_hostname;
```

Use of Zero Initialized Pointer\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3274
Status	New

The variable declared in psep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732 is not initialized when it is used by psep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2758	2818
Object	psep	psep

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2758.         psep = NULL;
....
2818.         memcpy(pbuf, psep + 1, plen);
```

Use of Zero Initialized Pointer\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3275

Status	New

The variable declared in psep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732 is not initialized when it is used by psep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2740	2818
Object	psep	psep

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2740.     const char *psep = NULL;
....
2818.         memcpy(pbuf, psep + 1, plen);
```

Use of Zero Initialized Pointer\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3276
Status	New

The variable declared in osep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732 is not initialized when it is used by osep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2767	2826
Object	osep	osep

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2767.         osep = NULL;
....
2826.         memcpy(obuf, osep + 1, olen);
```

Use of Zero Initialized Pointer\Path 48:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3277
Status	New

The variable declared in osep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732 is not initialized when it is used by osep at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2732.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2741	2826
Object	osep	osep

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2741.     const char *osep = NULL;
....
2826.         memcpy(obuf, osep + 1, olen);
```

Use of Zero Initialized Pointer\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3278
Status	New

The variable declared in conn_temp at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by dns_entry at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3281.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3395
Object	conn_temp	dns_entry

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3395.       DEBUGASSERT(conn->dns_entry == NULL);
```

Use of Zero Initialized Pointer\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3279
Status	New

The variable declared in endp at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 2989 is not initialized when it is used by dns_entry at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3281.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3055	3395
Object	endp	dns_entry

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3055.       char *endp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3395.       DEBUGASSERT(conn->dns_entry == NULL);
```

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=1000014&projectid=9&pathid=2529
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	1991	1991
Object	nickname	nickname

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static CURLcode nss_setup_connect(struct Curl_easy *data,

```
....
1991.       char *nickname = dup_nickname(data,
SSL_SET_OPTION(primary.clientcert));
```

Memory Leak\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2530
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	1999	1999
Object	nickname	nickname

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method	static CURLcode nss_setup_connect(struct Curl_easy *data,

```
....
1999.       char *nickname = dup_nickname(data,
SSL_SET_OPTION(primary.clientcert));
```

Memory Leak\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2531
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c

Line	2001	2001
Object	nickname	nickname

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static CURLcode nss_setup_connect(struct Curl_easy *data,

```
....
2001.       char *nickname = dup_nickname(data,
SSL_SET_OPTION(primary.clientcert));
```

Memory Leak\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2532
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	2040	2040
Object	nickname	nickname

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method static CURLcode nss_setup_connect(struct Curl_easy *data,

```
....
2040.       char *nickname = dup_nickname(data,
SSL_SET_OPTION(primary.clientcert));
```

Memory Leak\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2533
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	460	460
Object	wrap	wrap

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static CURLcode insert_wrapped_ptr(struct Curl_llist *list, void *ptr)

```
....
460.     struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

Memory Leak\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2534
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	460	460
Object	wrap	wrap

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static CURLcode insert_wrapped_ptr(struct Curl_llist *list, void *ptr)

```
....
460.     struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

Memory Leak\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2535
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	462	462
Object	wrap	wrap

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static CURLcode insert_wrapped_ptr(struct Curl_llist *list, void *ptr)

```
....
462.     struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

Memory Leak\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2536
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	462	462
Object	wrap	wrap

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	static CURLcode insert_wrapped_ptr(struct Curl_llist *list, void *ptr)

```
....
462.    struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

Memory Leak\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2537
Status	New

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2024-6874-TP.c	curl@@curl-curl-8_8_0-CVE-2024-6874-TP.c
Line	275	275
Object	c	c

Code Snippet

File Name	curl@@curl-curl-8_8_0-CVE-2024-6874-TP.c
Method	CURLcode Curl_idn_decode(const char *input, char **output)

```
....
275.      char *c = strdup(d);
```

Memory Leak\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2538
Status	New

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2024-6874-TP.c	curl@@curl-curl-8_8_0-CVE-2024-6874-TP.c
Line	294	294
Object	c	c

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2024-6874-TP.c
Method CURLcode Curl_idn_encode(const char *puny, char **output)

```
....
294.       char *c = strdup(d);
```

Memory Leak\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2539
Status	New

	Source	Destination
File	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c
Line	25	25
Object	nfc_dev	nfc_dev

Code Snippet
File Name DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c
Method NfcDevice* nfc_device_alloc() {

```
....
25.       NfcDevice* nfc_dev = malloc(sizeof(NfcDevice));
```

Memory Leak\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2540
Status	New

	Source	Destination
File	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c
Line	295	295

Object	kv	kv

Code Snippet
File Name DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c
Method bool nfc_device_load_mifare_df_key_settings(

```
....
295.                  MifareDesfireKeyVersion* kv =
malloc(sizeof(MifareDesfireKeyVersion));
```

Memory Leak\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2541
Status	New

	Source	Destination
File	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c
Line	1053	1053
Object	mem	mem

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c
Method _dwarf_special_no_dbg_error_malloc(void)

```
....
1053.      char *mem = (char *)malloc(len);
```

Memory Leak\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2542
Status	New

	Source	Destination
File	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c
Line	1053	1053
Object	mem	mem

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c
Method _dwarf_special_no_dbg_error_malloc(void)

```
....
1053.        char *mem = (char *)malloc(len);
```

Memory Leak\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2543
Status	New

	Source	Destination
File	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c
Line	1050	1050
Object	mem	mem

Code Snippet

File Name	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c
Method	_dwarf_special_no_dbg_error_malloc(void)

```
....
1050.        char *mem = (char *)malloc(len);
```

Memory Leak\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2544
Status	New

	Source	Destination
File	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c
Line	1050	1050
Object	mem	mem

Code Snippet

File Name	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c
Method	_dwarf_special_no_dbg_error_malloc(void)

```
....
1050.        char *mem = (char *)malloc(len);
```

Memory Leak\Path 17:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2545
Status	New

	Source	Destination
File	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Line	128	128
Object	addr	addr

Code Snippet
File Name dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Method new_address(const char *hostname_or_ip) {

```
....
128.        struct Address *addr = malloc(sizeof(struct Address));
```

Memory Leak\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2546
Status	New

	Source	Destination
File	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Line	171	171
Object	addr	addr

Code Snippet
File Name dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Method new_address(const char *hostname_or_ip) {

```
....
171.        struct Address *addr = malloc(
```

Memory Leak\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2547
Status	New

	Source	Destination
File	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Line	193	193
Object	addr	addr

Code Snippet
File Name dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Method new_address_sa(const struct sockaddr *sa, socklen_t sa_len) {

```
....
193.        struct Address *addr = malloc(offsetof(struct Address, data) + 
sa_len);
```

Memory Leak\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2548
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1123	1123
Object	filename	filename

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1123.        c->filename = strdup(file?file:"none"); /* copy the name just 
in case */
```

Memory Leak\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2549
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c

Line	798	798
Object	cred	cred

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
798.        BACKEND->cred = (struct Curl_schannel_cred *)
```

Memory Leak\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2550
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	917	917
Object	ctxt	ctxt

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
917.      BACKEND->ctxt = (struct Curl_schannel_ctxt *)
```

Memory Leak\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2551
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1031	1031
Object	decdata_buffer	decdata_buffer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c

Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1031.       BACKEND->decdata_buffer = malloc(BACKEND->decdata_length);
```

Memory Leak\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2552
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1043	1043
Object	encdata_buffer	encdata_buffer

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1043.       BACKEND->encdata_buffer = malloc(BACKEND->encdata_length);
```

Memory Leak\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2553
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1643	1643
Object	ptr	ptr

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1643.     ptr = (unsigned char *) malloc(data_len);
```

Memory Leak\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2554
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	798	798
Object	cred	cred

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
798.       BACKEND->cred = (struct Curl_schannel_cred *)
```

Memory Leak\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2555
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	917	917
Object	ctxt	ctxt

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
917.     BACKEND->ctxt = (struct Curl_schannel_ctxt *)
```

Memory Leak\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2556
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1031	1031
Object	decdata_buffer	decdata_buffer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1031.       BACKEND->decdata_buffer = malloc(BACKEND->decdata_length);
```

Memory Leak\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2557
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1043	1043
Object	encdata_buffer	encdata_buffer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1043.       BACKEND->encdata_buffer = malloc(BACKEND->encdata_length);
```

Memory Leak\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2558
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1643	1643

Object	ptr	ptr

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_send(struct Curl_easy *data, int sockindex,

```
....
1643.     ptr = (unsigned char *) malloc(data_len);
```

Memory Leak\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2559
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	102	102
Object	d	d

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method static CURLcode blobdup(struct curl_blob **dest,

```
....
102.       d = malloc(sizeof(struct curl_blob) + src->len);
```

Memory Leak\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2560
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	166	166
Object	CApath	CApath

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
166.     CLONE_STRING(CApath);
```

Memory Leak\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2561
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	167	167
Object	CAfile	CAfile

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
167.     CLONE_STRING(CAfile);
```

Memory Leak\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2562
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	168	168
Object	clientcert	clientcert

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
168.     CLONE_STRING(clientcert);
```

Memory Leak\Path 35:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2563
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	169	169
Object	random_file	random_file

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
169.     CLONE_STRING(random_file);
```

Memory Leak\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2564
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	170	170
Object	egdsocket	egdsocket

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
170.     CLONE_STRING(egdsocket);
```

Memory Leak\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2565
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	171	171
Object	cipher_list	cipher_list

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
171.     CLONE_STRING(cipher_list);
```

Memory Leak\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2566
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	172	172
Object	cipher_list13	cipher_list13

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
172.     CLONE_STRING(cipher_list13);
```

Memory Leak\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2567
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	173	173

Object	pinned_key	pinned_key

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
173.     CLONE_STRING(pinned_key);
```

Memory Leak\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2568
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	174	174
Object	curves	curves

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method Curl_clone_primary_ssl_config(struct ssl_primary_config *source,

```
....
174.     CLONE_STRING(curves);
```

Memory Leak\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2569
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	698	698
Object	session	session

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_ssl_initsessions(struct Curl_easy *data, size_t amount)

```
....
698.    session = calloc(amount, sizeof(struct Curl_ssl_session));
```

Memory Leak\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2570
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	766	766
Object	table	table

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
766.    table = calloc((size_t) num, sizeof(struct curl_slist *));
```

Memory Leak\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2571
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	871	871
Object	stripped_pem	stripped_pem

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	static CURLcode pubkey_pem_to_der(const char *pem,

```
....
871.    stripped_pem = malloc(pem_len - pem_count + 1);
```

Memory Leak\Path 44:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2572
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	926	926
Object	sha256sumdigest	sha256sumdigest

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
926.       sha256sumdigest = malloc(CURL_SHA256_DIGEST_LENGTH);
```

Memory Leak\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2573
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	947	947
Object	pinkeycopy	pinkeycopy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
947.       pinkeycopy = malloc(pinkeylen);
```

Memory Leak\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2574
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	1015	1015
Object	buf	buf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1015.       buf = malloc(size + 1);
```

Memory Leak\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2575
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	201	201
Object	tn	tn

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method CURLcode init_telnet(struct Curl_easy *data)

```
....
201.    tn = calloc(1, sizeof(struct TELNET));
```

Memory Leak\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2576
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	105	105

Object	mq	mq

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_setup_conn(struct Curl_easy *data,

```
....
105.     mq = calloc(1, sizeof(struct MQTT));
```

Memory Leak\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2577
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Line	651	651
Object	apoptimestamp	apoptimestamp

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_state_servergreet_resp(struct Curl_easy *data,

```
....
651.          pop3c->apoptimestamp = (char *)calloc(1, timestamplen +
1);
```

Memory Leak\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2578
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Line	1066	1066
Object	pop3	pop3

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_init(struct Curl_easy *data)

```
....
1066.     pop3 = data->req.p.pop3 = calloc(sizeof(struct POP3), 1);
```

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=1000014&projectid=9&pathid=2143
Status	New

Calling free() (line 206) on a variable that was not dynamically allocated (line 206) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	264	264
Object	stringp	stringp

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
264.       free(stringp);
```

MemoryFree on StackVariable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2144
Status	New

Calling free() (line 206) on a variable that was not dynamically allocated (line 206) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	326	326
Object	p	p

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
326.            free(p);
```

MemoryFree on StackVariable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2145
Status	New

Calling free() (line 206) on a variable that was not dynamically allocated (line 206) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	327	327
Object	cmd	cmd

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
327.            free(cmd);
```

MemoryFree on StackVariable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2146
Status	New

Calling free() (line 601) on a variable that was not dynamically allocated (line 601) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	629	629
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	static void do_sec_send(struct Curl_easy *data, struct connectdata *conn,

```
....
629.        free(buffer);
```

MemoryFree on StackVariable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2147
Status	New

Calling free() (line 601) on a variable that was not dynamically allocated (line 601) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	644	644
Object	cmd_buffer	cmd_buffer

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	static void do_sec_send(struct Curl_easy *data, struct connectdata *conn,

```
....
644.        free(cmd_buffer);
```

MemoryFree on StackVariable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2148
Status	New

Calling free() (line 601) on a variable that was not dynamically allocated (line 601) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	652	652
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c

Method	static void do_sec_send(struct Curl_easy *data, struct connectdata *conn,

```
....
652.     free(buffer);
```

MemoryFree on StackVariable\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2149
Status	New

Calling free() (line 686) on a variable that was not dynamically allocated (line 686) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	710	710
Object	buf	buf

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
710.       free(buf);
```

MemoryFree on StackVariable\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2150
Status	New

Calling free() (line 686) on a variable that was not dynamically allocated (line 686) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	718	718
Object	buf	buf

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
718.         free(buf);
```

MemoryFree on StackVariable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2151
Status	New

Calling free() (line 686) on a variable that was not dynamically allocated (line 686) in file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	739	739
Object	buf	buf

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	int Curl_sec_read_msg(struct Curl_easy *data, struct connectdata *conn,

```
....
739.      free(buf);
```

MemoryFree on StackVariable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2152
Status	New

Calling free() (line 1514) on a variable that was not dynamically allocated (line 1514) in file curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1605	1605
Object	tempstore	tempstore

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	static int cookie_output(struct Curl_easy *data,

```
....
1605.     free(tempstore);
```

MemoryFree on StackVariable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2153
Status	New

Calling free() (line 1609) on a variable that was not dynamically allocated (line 1609) in file curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1632	1632
Object	line	line

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method static struct curl_slist *cookie_list(struct Curl_easy *data)

```
....
1632.           free(line);
```

MemoryFree on StackVariable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2154
Status	New

Calling free() (line 827) on a variable that was not dynamically allocated (line 827) in file curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Line	835	835
Object	dns	dns

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Method static void freednsentry(void *freethis)

```
....
835.        free(dns);
```

MemoryFree on StackVariable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2155
Status	New

Calling free() (line 418) on a variable that was not dynamically allocated (line 418) in file curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	752	752
Object	cert_store_path	cert_store_path

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
752.            free(cert_store_path);
```

MemoryFree on StackVariable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2156
Status	New

Calling free() (line 418) on a variable that was not dynamically allocated (line 418) in file curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	756	756
Object	cert_store_path	cert_store_path

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
756.            free(cert_store_path);
```

MemoryFree on StackVariable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2157
Status	New

Calling free() (line 418) on a variable that was not dynamically allocated (line 418) in file curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	752	752
Object	cert_store_path	cert_store_path

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
752.              free(cert_store_path);
```

MemoryFree on StackVariable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2158
Status	New

Calling free() (line 418) on a variable that was not dynamically allocated (line 418) in file curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	756	756
Object	cert_store_path	cert_store_path

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
756.          free(cert_store_path);
```

MemoryFree on StackVariable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2159
Status	New

Calling free() (line 543) on a variable that was not dynamically allocated (line 543) in file curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	560	560
Object	ptr	ptr

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method	static CURLcode mqtt_doing(struct Curl_easy *data, bool *done)

```
....
560.       free(ptr);
```

MemoryFree on StackVariable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2160
Status	New

Calling free() (line 247) on a variable that was not dynamically allocated (line 247) in file curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	287	287
Object	topic	topic

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method	static CURLcode mqtt_subscribe(struct Curl_easy *data)

```
....
287.     free(topic);
```

MemoryFree on StackVariable\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2161
Status	New

Calling free() (line 326) on a variable that was not dynamically allocated (line 326) in file curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	375	375
Object	topic	topic

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method	static CURLcode mqtt_publish(struct Curl_easy *data)

```
....
375.     free(topic);
```

MemoryFree on StackVariable\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2162
Status	New

Calling free() (line 355) on a variable that was not dynamically allocated (line 355) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	470	470
Object	data	data

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_close(struct Curl_easy **datap)

```
....
470.     free(data);
```

MemoryFree on StackVariable\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2163
Status	New

Calling free() (line 1850) on a variable that was not dynamically allocated (line 1850) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	1887	1887
Object	zoneid	zoneid

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static void zonefrom_url(CURLU *uh, struct Curl_easy *data,

```
....
1887.       free(zoneid);
```

MemoryFree on StackVariable\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2164
Status	New

Calling free() (line 1894) on a variable that was not dynamically allocated (line 1894) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	1977	1977
Object	url	url

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....
1977.          free(url);
```

MemoryFree on StackVariable\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2165
Status	New

Calling free() (line 2347) on a variable that was not dynamically allocated (line 2347) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2455	2455
Object	portptr	portptr

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode parse_proxy(struct Curl_easy *data,

```
....
2455.        free(portptr);
```

MemoryFree on StackVariable\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2166
Status	New

Calling free() (line 2347) on a variable that was not dynamically allocated (line 2347) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2493	2493
Object	proxyuser	proxyuser

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode parse_proxy(struct Curl_easy *data,

```
....
2493.     free(proxyuser);
```

MemoryFree on StackVariable\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2167
Status	New

Calling free() (line 2347) on a variable that was not dynamically allocated (line 2347) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2495	2495
Object	scheme	scheme

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode parse_proxy(struct Curl_easy *data,

```
....
2495.     free(scheme);
```

MemoryFree on StackVariable\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2168
Status	New

Calling free() (line 3090) on a variable that was not dynamically allocated (line 3090) in file curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3121	3121
Object	hostname_to_match	hostname_to_match

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode parse_connect_to_string(struct Curl_easy *data,

```
....
3121.        free(hostname_to_match);
```

MemoryFree on StackVariable\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2169
Status	New

Calling free() (line 299) on a variable that was not dynamically allocated (line 299) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	343	343
Object	authorization	authorization

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	static CURLcode http_output_basic(struct Curl_easy *data, bool proxy)

```
....
343.     free(authorization);
```

MemoryFree on StackVariable\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2170
Status	New

Calling free() (line 299) on a variable that was not dynamically allocated (line 299) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	350	350
Object	out	out

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	static CURLcode http_output_basic(struct Curl_easy *data, bool proxy)

```
....
350.     free(out);
```

MemoryFree on StackVariable\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2171
Status	New

Calling free() (line 2079) on a variable that was not dynamically allocated (line 2079) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	2108	2108
Object	cookiehost	cookiehost

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method CURLcode Curl_http_host(struct Curl_easy *data, struct connectdata *conn)

```
....
2108.         free(cookiehost);
```

MemoryFree on StackVariable\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2172
Status	New

Calling free() (line 2173) on a variable that was not dynamically allocated (line 2173) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	2241	2241
Object	url	url

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method CURLcode Curl_http_target(struct Curl_easy *data,

```
....
2241.       free(url);
```

MemoryFree on StackVariable\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2173
Status	New

Calling free() (line 2967) on a variable that was not dynamically allocated (line 2967) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	3052	3052
Object	pq	pq

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	CURLcode Curl_http(struct Curl_easy *data, bool *done)

```
....
3052.       free(pq);
```

MemoryFree on StackVariable\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2174
Status	New

Calling free() (line 2967) on a variable that was not dynamically allocated (line 2967) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	3201	3201
Object	altused	altused

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	CURLcode Curl_http(struct Curl_easy *data, bool *done)

```
....
3201.     free(altused);
```

MemoryFree on StackVariable\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2175
Status	New

Calling free() (line 3382) on a variable that was not dynamically allocated (line 3382) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	3429	3429
Object	contenttype	contenttype

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method CURLcode Curl_http_header(struct Curl_easy *data, struct connectdata *conn,

```
....
3429.         free(contenttype);
```

MemoryFree on StackVariable\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2176
Status	New

Calling free() (line 3382) on a variable that was not dynamically allocated (line 3382) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	3591	3591
Object	auth	auth

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method CURLcode Curl_http_header(struct Curl_easy *data, struct connectdata *conn,

```
....
3591.        free(auth);
```

MemoryFree on StackVariable\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2177
Status	New

Calling free() (line 3382) on a variable that was not dynamically allocated (line 3382) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	3609	3609
Object	persistentauth	persistentauth

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	CURLcode Curl_http_header(struct Curl_easy *data, struct connectdata *conn,

```
....
3609.          free(persistentauth);
```

MemoryFree on StackVariable\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2178
Status	New

Calling free() (line 3382) on a variable that was not dynamically allocated (line 3382) in file curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	3622	3622
Object	location	location

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	CURLcode Curl_http_header(struct Curl_easy *data, struct connectdata *conn,

```
....
3622.        free(location);
```

MemoryFree on StackVariable\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2179
Status	New

Calling free() (line 1574) on a variable that was not dynamically allocated (line 1574) in file curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1668	1668
Object	tempstore	tempstore

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1668.     free(tempstore);
```

MemoryFree on StackVariable\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2180
Status	New

Calling free() (line 1574) on a variable that was not dynamically allocated (line 1574) in file curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1674	1674
Object	tempstore	tempstore

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1674.     free(tempstore);
```

MemoryFree on StackVariable\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2181
Status	New

Calling free() (line 1678) on a variable that was not dynamically allocated (line 1678) in file curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1700	1700
Object	line	line

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static struct curl_slist *cookie_list(struct Curl_easy *data)

```
....
1700.           free(line);
```

MemoryFree on StackVariable\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2182
Status	New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	493	493
Object	slot_name	slot_name

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static CURLcode nss_create_object(struct ssl_connect_data *connssl,

```
....
493.     free(slot_name);
```

MemoryFree on StackVariable\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2183
Status	New

Calling free() (line 537) on a variable that was not dynamically allocated (line 537) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	543	543
Object	wrap	wrap

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static void nss_destroy_object(void *user, void *ptr)

```
....
543.     free(wrap);
```

MemoryFree on StackVariable\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2184
Status	New

Calling free() (line 547) on a variable that was not dynamically allocated (line 547) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	553	553
Object	wrap	wrap

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static void nss_destroy_crl_item(void *user, void *ptr)

```
....
553.     free(wrap);
```

MemoryFree on StackVariable\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2185
Status	New

Calling free() (line 556) on a variable that was not dynamically allocated (line 556) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	585	585
Object	nickname	nickname

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c

Method static CURLcode nss_load_cert(struct ssl_connect_data *ssl,

```
....
585.         free(nickname);
```

MemoryFree on StackVariable\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2186
Status	New

Calling free() (line 1297) on a variable that was not dynamically allocated (line 1297) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	1311	1311
Object	config_string	config_string

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c

Method static CURLcode nss_load_module(SECMODModule **pmod, const char *library,

```
....
1311.      free(config_string);
```

MemoryFree on StackVariable\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2187
Status	New

Calling free() (line 1341) on a variable that was not dynamically allocated (line 1341) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	1361	1361
Object	certpath	certpath

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static CURLcode nss_init_core(struct Curl_easy *data, const char *cert_dir)

```
....
1361.        free(certpath);
```

MemoryFree on StackVariable\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2188
Status	New

Calling free() (line 1638) on a variable that was not dynamically allocated (line 1638) in file curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	1707	1707
Object	fullpath	fullpath

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static CURLcode nss_load_ca_certificates(struct Curl_easy *data,

```
....
1707.          free(fullpath);
```

MemoryFree on StackVariable\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2189
Status	New

Calling free() (line 355) on a variable that was not dynamically allocated (line 355) in file curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	470	470
Object	data	data

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_close(struct Curl_easy **datap)

```
....
470.     free(data);
```

MemoryFree on StackVariable\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2190
Status	New

Calling free() (line 1850) on a variable that was not dynamically allocated (line 1850) in file curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	1887	1887
Object	zoneid	zoneid

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static void zonefrom_url(CURLU *uh, struct Curl_easy *data,

```
....
1887.       free(zoneid);
```

MemoryFree on StackVariable\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2191
Status	New

Calling free() (line 1894) on a variable that was not dynamically allocated (line 1894) in file curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	1977	1977
Object	url	url

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static CURLcode parseurlandfillconn(struct Curl_easy *data,

```
....
1977.         free(url);
```

MemoryFree on StackVariable\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2192
Status	New

Calling free() (line 2347) on a variable that was not dynamically allocated (line 2347) in file curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c may result with a crash.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2455	2455
Object	portptr	portptr

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static CURLcode parse_proxy(struct Curl_easy *data,

```
....
2455.       free(portptr);
```

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=1000014&projectid=9&pathid=28
Status	New

The size of the buffer used by *get_localhost6 in ipv6, at line 465 of curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost6 passes to ipv6, at line 465 of curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c
Line	483	483
Object	ipv6	ipv6

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c
Method static struct Curl_addrinfo *get_localhost6(int port)

```
....
483.     memcpy(&sa6.sin6_addr, ipv6, sizeof(ipv6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=29
Status	New

The size of the buffer used by *get_localhost in ipv4, at line 502 of curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost passes to ipv4, at line 502 of curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination

File	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c
Line	520	520
Object	ipv4	ipv4

Code Snippet
File Name	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c
Method	static struct Curl_addrinfo *get_localhost(int port)

```
....
520.     memcpy(&sa.sin_addr, &ipv4, sizeof(ipv4));
```

Buffer Overflow boundcpy WrongSizeParam\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=30
Status	New

The size of the buffer used by *get_localhost6 in ipv6, at line 465 of curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost6 passes to ipv6, at line 465 of curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c
Line	483	483
Object	ipv6	ipv6

Code Snippet
File Name	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c
Method	static struct Curl_addrinfo *get_localhost6(int port)

```
....
483.     memcpy(&sa6.sin6_addr, ipv6, sizeof(ipv6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=31
Status	New

The size of the buffer used by *get_localhost in ipv4, at line 502 of curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost passes to ipv4, at line 502 of curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c
Line	517	517
Object	ipv4	ipv4

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c
Method	static struct Curl_addrinfo *get_localhost(int port)

```
....
517.     memcpy(&sa.sin_addr, &ipv4, sizeof(ipv4));
```

Buffer Overflow boundcpy WrongSizeParam\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=32
Status	New

The size of the buffer used by *get_localhost6 in ipv6, at line 465 of curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost6 passes to ipv6, at line 465 of curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c
Line	483	483
Object	ipv6	ipv6

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c
Method	static struct Curl_addrinfo *get_localhost6(int port)

```
....
483.     memcpy(&sa6.sin6_addr, ipv6, sizeof(ipv6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=33
Status	New

The size of the buffer used by *get_localhost in ipv4, at line 502 of curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost passes to ipv4, at line 502 of curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c
Line	517	517
Object	ipv4	ipv4

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c
Method static struct Curl_addrinfo *get_localhost(int port)

```
....
517.     memcpy(&sa.sin_addr, &ipv4, sizeof(ipv4));
```

Buffer Overflow boundcpy WrongSizeParam\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=34
Status	New

The size of the buffer used by *get_localhost6 in ipv6, at line 467 of curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost6 passes to ipv6, at line 467 of curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c
Line	485	485
Object	ipv6	ipv6

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c
Method static struct Curl_addrinfo *get_localhost6(int port, const char *name)

```
....
485.     memcpy(&sa6.sin6_addr, ipv6, sizeof(ipv6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=35
Status	New

The size of the buffer used by *get_localhost in ipv4, at line 504 of curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost passes to ipv4, at line 504 of curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c
Line	519	519
Object	ipv4	ipv4

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c
Method static struct Curl_addrinfo *get_localhost(int port, const char *name)

```
....
519.    memcpy(&sa.sin_addr, &ipv4, sizeof(ipv4));
```

Buffer Overflow boundcpy WrongSizeParam\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=36
Status	New

The size of the buffer used by multi_addtimeout in stamp, at line 3469 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_addtimeout passes to stamp, at line 3469 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Line	3482	3482
Object	stamp	stamp

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Method multi_addtimeout(struct Curl_easy *data,

```
....
3482.    memcpy(&node->time, stamp, sizeof(*stamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=37
Status	New

The size of the buffer used by *get_localhost6 in ipv6, at line 488 of curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost6 passes to ipv6, at line 488 of curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c
Line	506	506
Object	ipv6	ipv6

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c
Method	static struct Curl_addrinfo *get_localhost6(int port, const char *name)

```
....
506.    memcpy(&sa6.sin6_addr, ipv6, sizeof(ipv6));
```

Buffer Overflow boundcpy WrongSizeParam\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=38
Status	New

The size of the buffer used by *get_localhost in ipv4, at line 525 of curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *get_localhost passes to ipv4, at line 525 of curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c
Line	540	540
Object	ipv4	ipv4

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c
Method	static struct Curl_addrinfo *get_localhost(int port, const char *name)

```
....
540.    memcpy(&sa.sin_addr, &ipv4, sizeof(ipv4));
```

Buffer Overflow boundcpy WrongSizeParam\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=39

Status	New

The size of the buffer used by multi_addtimeout in stamp, at line 3545 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_addtimeout passes to stamp, at line 3545 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Line	3558	3558
Object	stamp	stamp

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Method multi_addtimeout(struct Curl_easy *data,

```
....
3558.     memcpy(&node->time, stamp, sizeof(*stamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=40
Status	New

The size of the buffer used by multi_addtimeout in stamp, at line 3542 of curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_addtimeout passes to stamp, at line 3542 of curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c
Line	3555	3555
Object	stamp	stamp

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c
Method multi_addtimeout(struct Curl_easy *data,

```
....
3555.     memcpy(&node->time, stamp, sizeof(*stamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=41
Status	New

The size of the buffer used by singlesocket in ->, at line 2935 of curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that singlesocket passes to ->, at line 2935 of curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c
Line	3081	3081
Object	->	->

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
3081.    memcpy(&data->last_poll, &cur_poll, sizeof(data->last_poll));
```

Buffer Overflow boundcpy WrongSizeParam\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=42
Status	New

The size of the buffer used by multi_addtimeout in stamp, at line 3555 of curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_addtimeout passes to stamp, at line 3555 of curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c
Line	3568	3568
Object	stamp	stamp

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c
Method multi_addtimeout(struct Curl_easy *data,

```
....
3568.    memcpy(&node->time, stamp, sizeof(*stamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 16:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=43
Status	New

The size of the buffer used by singlesocket in ->, at line 2926 of curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that singlesocket passes to ->, at line 2926 of curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c
Line	3072	3072
Object	->	->

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
3072.     memcpy(&data->last_poll, &cur_poll, sizeof(data->last_poll));
```

Buffer Overflow boundcpy WrongSizeParam\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=44
Status	New

The size of the buffer used by multi_addtimeout in stamp, at line 3546 of curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_addtimeout passes to stamp, at line 3546 of curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c
Line	3559	3559
Object	stamp	stamp

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c
Method multi_addtimeout(struct Curl_easy *data,

```
....
3559.     memcpy(&node->time, stamp, sizeof(*stamp));
```

Buffer Overflow boundcpy WrongSizeParam\Path 18:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=45
Status	New

The size of the buffer used by _dwarf_internal_global_formref_b in Dwarf_Sig8, at line 729 of davea42@@libdwarf-code-v0.8.0-CVE-2022-34299-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _dwarf_internal_global_formref_b passes to Dwarf_Sig8, at line 729 of davea42@@libdwarf-code-v0.8.0-CVE-2022-34299-FP.c, to overwrite the target buffer.

	Source	Destination
File	davea42@@libdwarf-code-v0.8.0-CVE-2022-34299-FP.c	davea42@@libdwarf-code-v0.8.0-CVE-2022-34299-FP.c
Line	902	902
Object	Dwarf_Sig8	Dwarf_Sig8

Code Snippet

File Name davea42@@libdwarf-code-v0.8.0-CVE-2022-34299-FP.c

Method _dwarf_internal_global_formref_b(Dwarf_Attribute attr,

```
....
902.            memcpy(&sig8,attr->ar_debug_ptr,sizeof(Dwarf_Sig8));
```

Buffer Overflow boundcpy WrongSizeParam\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=46
Status	New

The size of the buffer used by *create_reference in cJSON, at line 1921 of DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *create_reference passes to cJSON, at line 1921 of DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c
Line	1935	1935
Object	cJSON	cJSON

Code Snippet

File Name DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c

Method static cJSON *create_reference(const cJSON *item, const internal_hooks * const hooks)

```
....
1935.       memcpy(reference, item, sizeof(cJSON));
```

Buffer Overflow boundcpy WrongSizeParam\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=47
Status	New

The size of the buffer used by *create_reference in cJSON, at line 1929 of DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *create_reference passes to cJSON, at line 1929 of DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c
Line	1943	1943
Object	cJSON	cJSON

Code Snippet

File Name	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c
Method	static cJSON *create_reference(const cJSON *item, const internal_hooks * const hooks)

```
....
1943.      memcpy(reference, item, sizeof(cJSON));
```

Buffer Overflow boundcpy WrongSizeParam\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=48
Status	New

The size of the buffer used by *create_reference in cJSON, at line 1931 of DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *create_reference passes to cJSON, at line 1931 of DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c
Line	1945	1945
Object	cJSON	cJSON

Code Snippet

File Name	DaveGamble@@cJSON-v1.7.15-CVE-2024-31755-TP.c
Method	static cJSON *create_reference(const cJSON *item, const internal_hooks * const hooks)

```
....
1945.     memcpy(reference, item, sizeof(cJSON));
```

Buffer Overflow boundcpy WrongSizeParam\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=49
Status	New

The size of the buffer used by *create_reference in cJSON, at line 1935 of DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *create_reference passes to cJSON, at line 1935 of DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c
Line	1949	1949
Object	cJSON	cJSON

Code Snippet

File Name	DaveGamble@@cJSON-v1.7.16-CVE-2024-31755-TP.c
Method	static cJSON *create_reference(const cJSON *item, const internal_hooks * const hooks)

```
....
1949.     memcpy(reference, item, sizeof(cJSON));
```

Buffer Overflow boundcpy WrongSizeParam\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=50
Status	New

The size of the buffer used by *create_reference in cJSON, at line 1940 of DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that *create_reference passes to cJSON, at line 1940 of DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c, to overwrite the target buffer.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c
Line	1954	1954
Object	cJSON	cJSON

Code Snippet

File Name	DaveGamble@@cJSON-v1.7.17-CVE-2024-31755-TP.c
Method	static cJSON *create_reference(const cJSON *item, const internal_hooks * const hooks)

```
....
1954.       memcpy(reference, item, sizeof(cJSON));
```

Buffer Overflow boundcpy WrongSizeParam\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=51
Status	New

The size of the buffer used by Curl_connect in SingleRequest, at line 4053 of curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_connect passes to SingleRequest, at line 4053 of curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	4064	4064
Object	SingleRequest	SingleRequest

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_connect(struct Curl_easy *data,

```
....
4064.     memset(&data->req, 0, sizeof(struct SingleRequest));
```

Buffer Overflow boundcpy WrongSizeParam\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=52
Status	New

The size of the buffer used by nss_init_core in initparams, at line 1341 of curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nss_init_core passes to initparams, at line 1341 of curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	1350	1350
Object	initparams	initparams

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static CURLcode nss_init_core(struct Curl_easy *data, const char *cert_dir)

```
....
1350.     memset((void *) &initparams, '\0', sizeof(initparams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=53
Status	New

The size of the buffer used by Curl_connect in SingleRequest, at line 4053 of curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_connect passes to SingleRequest, at line 4053 of curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	4064	4064
Object	SingleRequest	SingleRequest

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	CURLcode Curl_connect(struct Curl_easy *data,

```
....
4064.     memset(&data->req, 0, sizeof(struct SingleRequest));
```

Buffer Overflow boundcpy WrongSizeParam\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=54
Status	New

The size of the buffer used by nss_init_core in initparams, at line 1341 of curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nss_init_core passes to initparams, at line 1341 of curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	1350	1350

Object	initparams	initparams

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static CURLcode nss_init_core(struct Curl_easy *data, const char *cert_dir)

```
....
1350.     memset((void *) &initparams, '\0', sizeof(initparams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=55
Status	New

The size of the buffer used by Curl_connect in SingleRequest, at line 4084 of curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_connect passes to SingleRequest, at line 4084 of curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	4095	4095
Object	SingleRequest	SingleRequest

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method CURLcode Curl_connect(struct Curl_easy *data,

```
....
4095.     memset(&data->req, 0, sizeof(struct SingleRequest));
```

Buffer Overflow boundcpy WrongSizeParam\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=56
Status	New

The size of the buffer used by nss_init_core in initparams, at line 1343 of curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nss_init_core passes to initparams, at line 1343 of curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c

Line	1352	1352
Object	initparams	initparams

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static CURLcode nss_init_core(struct Curl_easy *data, const char *cert_dir)

```
....
1352.    memset((void *) &initparams, '\0', sizeof(initparams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=57
Status	New

The size of the buffer used by Curl_connect in SingleRequest, at line 4114 of curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_connect passes to SingleRequest, at line 4114 of curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Line	4125	4125
Object	SingleRequest	SingleRequest

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Method CURLcode Curl_connect(struct Curl_easy *data,

```
....
4125.    memset(&data->req, 0, sizeof(struct SingleRequest));
```

Buffer Overflow boundcpy WrongSizeParam\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=58
Status	New

The size of the buffer used by ssh_statemach_act in LIBSSH2_SFTP_ATTRIBUTES, at line 899 of curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to LIBSSH2_SFTP_ATTRIBUTES, at line 899 of curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination

File	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c
Line	1522	1522
Object	LIBSSH2_SFTP_ATTRIBUTES	LIBSSH2_SFTP_ATTRIBUTES

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
1522.              memset(&sshp->quote_attrs, 0,
sizeof(LIBSSH2_SFTP_ATTRIBUTES));
```

Buffer Overflow boundcpy WrongSizeParam\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=59
Status	New

The size of the buffer used by ssh_statemach_act in stat, at line 899 of curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to stat, at line 899 of curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c
Line	2708	2708
Object	stat	stat

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2708.         memset(&sb, 0, sizeof(struct stat));
```

Buffer Overflow boundcpy WrongSizeParam\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=60
Status	New

The size of the buffer used by ssh_statemach_act in ssh_conn, at line 899 of curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to ssh_conn, at line 899 of curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c
Line	2947	2947
Object	ssh_conn	ssh_conn

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2947.         memset(sshc, 0, sizeof(struct ssh_conn));
```

Buffer Overflow boundcpy WrongSizeParam\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=61
Status	New

The size of the buffer used by nss_init_core in initparams, at line 1360 of curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that nss_init_core passes to initparams, at line 1360 of curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	1369	1369
Object	initparams	initparams

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	static CURLcode nss_init_core(struct Curl_easy *data, const char *cert_dir)

```
....
1369.     memset((void *) &initparams, '\0', sizeof(initparams));
```

Buffer Overflow boundcpy WrongSizeParam\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=62
Status	New

The size of the buffer used by Curl_connect in SingleRequest, at line 4121 of curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that Curl_connect passes to SingleRequest, at line 4121 of curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Line	4132	4132
Object	SingleRequest	SingleRequest

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Method	CURLcode Curl_connect(struct Curl_easy *data,

```
....
4132.     memset(&data->req, 0, sizeof(struct SingleRequest));
```

Buffer Overflow boundcpy WrongSizeParam\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=63
Status	New

The size of the buffer used by ssh_statemach_act in LIBSSH2_SFTP_ATTRIBUTES, at line 898 of curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to LIBSSH2_SFTP_ATTRIBUTES, at line 898 of curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c
Line	1521	1521
Object	LIBSSH2_SFTP_ATTRIBUTES	LIBSSH2_SFTP_ATTRIBUTES

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
1521.             memset(&sshp->quote_attrs, 0,
sizeof(LIBSSH2_SFTP_ATTRIBUTES));
```

Buffer Overflow boundcpy WrongSizeParam\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=64
Status	New

The size of the buffer used by ssh_statemach_act in stat, at line 898 of curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to stat, at line 898 of curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c
Line	2707	2707
Object	stat	stat

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c
Method static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2707.        memset(&sb, 0, sizeof(struct stat));
```

Buffer Overflow boundcpy WrongSizeParam\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=65
Status	New

The size of the buffer used by ssh_statemach_act in ssh_conn, at line 898 of curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to ssh_conn, at line 898 of curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c
Line	2946	2946
Object	ssh_conn	ssh_conn

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2023-28319-TP.c
Method static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2946.        memset(sshc, 0, sizeof(struct ssh_conn));
```

Buffer Overflow boundcpy WrongSizeParam\Path 39:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=66
Status	New

The size of the buffer used by ssh_statemach_act in LIBSSH2_SFTP_ATTRIBUTES, at line 955 of curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to LIBSSH2_SFTP_ATTRIBUTES, at line 955 of curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c
Line	1578	1578
Object	LIBSSH2_SFTP_ATTRIBUTES	LIBSSH2_SFTP_ATTRIBUTES

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
1578.                memset(&sshp->quote_attrs, 0,
sizeof(LIBSSH2_SFTP_ATTRIBUTES));
```

Buffer Overflow boundcpy WrongSizeParam\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=67
Status	New

The size of the buffer used by ssh_statemach_act in stat, at line 955 of curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to stat, at line 955 of curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c
Line	2768	2768
Object	stat	stat

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2768.          memset(&sb, 0, sizeof(struct stat));
```

Buffer Overflow boundcpy WrongSizeParam\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=68
Status	New

The size of the buffer used by ssh_statemach_act in ssh_conn, at line 955 of curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to ssh_conn, at line 955 of curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c
Line	3007	3007
Object	ssh_conn	ssh_conn

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
3007.        memset(sshc, 0, sizeof(struct ssh_conn));
```

Buffer Overflow boundcpy WrongSizeParam\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=69
Status	New

The size of the buffer used by curl_multi_add_handle in ->, at line 462 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_multi_add_handle passes to ->, at line 462 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Line	525	525
Object	->	->

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Method	CURLMcode curl_multi_add_handle(struct Curl_multi *multi,

```
....
525.    memset(&multi->timer_lastcall, 0, sizeof(multi-
>timer_lastcall));
```

Buffer Overflow boundcpy WrongSizeParam\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=70
Status	New

The size of the buffer used by multi_socket in ->, at line 3108 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_socket passes to ->, at line 3108 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Line	3181	3181
Object	->	->

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Method	static CURLMcode multi_socket(struct Curl_multi *multi,

```
....
3181.       memset(&multi->timer_lastcall, 0, sizeof(multi-
>timer_lastcall));
```

Buffer Overflow boundcpy WrongSizeParam\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=71
Status	New

The size of the buffer used by ssh_statemach_act in LIBSSH2_SFTP_ATTRIBUTES, at line 954 of curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to LIBSSH2_SFTP_ATTRIBUTES, at line 954 of curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c
Line	1577	1577
Object	LIBSSH2_SFTP_ATTRIBUTES	LIBSSH2_SFTP_ATTRIBUTES

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
1577.              memset(&sshp->quote_attrs, 0,
sizeof(LIBSSH2_SFTP_ATTRIBUTES));
```

Buffer Overflow boundcpy WrongSizeParam\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=72
Status	New

The size of the buffer used by ssh_statemach_act in stat, at line 954 of curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to stat, at line 954 of curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c
Line	2767	2767
Object	stat	stat

Code Snippet
File Name   curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c
Method   static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2767.          memset(&sb, 0, sizeof(struct stat));
```

Buffer Overflow boundcpy WrongSizeParam\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=73
Status	New

The size of the buffer used by ssh_statemach_act in ssh_conn, at line 954 of curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to ssh_conn, at line 954 of curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c
Line	3006	3006
Object	ssh_conn	ssh_conn

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2023-28319-TP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
3006.        memset(sshc, 0, sizeof(struct ssh_conn));
```

Buffer Overflow boundcpy WrongSizeParam\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=74
Status	New

The size of the buffer used by curl_multi_add_handle in ->, at line 513 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that curl_multi_add_handle passes to ->, at line 513 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Line	576	576
Object	->	->

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Method	CURLMcode curl_multi_add_handle(struct Curl_multi *multi,

```
....
576.    memset(&multi->timer_lastcall, 0, sizeof(multi-
>timer_lastcall));
```

Buffer Overflow boundcpy WrongSizeParam\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=75
Status	New

The size of the buffer used by multi_socket in ->, at line 3173 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that multi_socket passes to ->, at line 3173 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Line	3249	3249
Object	->	->

Code Snippet	
File Name	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Method	static CURLMcode multi_socket(struct Curl_multi *multi,

```
....
3249.        memset(&multi->timer_lastcall, 0, sizeof(multi-
>timer_lastcall));
```

Buffer Overflow boundcpy WrongSizeParam\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=76
Status	New

The size of the buffer used by ssh_statemach_act in LIBSSH2_SFTP_ATTRIBUTES, at line 969 of curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to LIBSSH2_SFTP_ATTRIBUTES, at line 969 of curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c	curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c
Line	1592	1592
Object	LIBSSH2_SFTP_ATTRIBUTES	LIBSSH2_SFTP_ATTRIBUTES

Code Snippet	
File Name	curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c
Method	static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
1592.            memset(&sshp->quote_attrs, 0,
sizeof(LIBSSH2_SFTP_ATTRIBUTES));
```

Buffer Overflow boundcpy WrongSizeParam\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=77
Status	New

The size of the buffer used by ssh_statemach_act in stat, at line 969 of curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that ssh_statemach_act passes to stat, at line 969 of curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c, to overwrite the target buffer.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2023-	curl@@curl-curl-8_1_0-CVE-2023-

	28319-FP.c	28319-FP.c
Line	2781	2781
Object	stat	stat

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2023-28319-FP.c
Method static CURLcode ssh_statemach_act(struct Curl_easy *data, bool *block)

```
....
2781.         memset(&sb, 0, sizeof(struct stat));
```

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=1000014&projectid=9&pathid=342
Status	New

The function data_len in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c at line 1610 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	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1643	1643
Object	data_len	data_len

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_send(struct Curl_easy *data, int sockindex,

```
....
1643.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=343
Status	New

The function data_len in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c at line 1610 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	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1643	1643
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1643.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=344
Status	New

The function outlen in curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c at line 779 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	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	792	792
Object	outlen	outlen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
792.     output = malloc(outlen);
```

Wrong Size t Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=345
Status	New

The function pinkeylen in curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c at line 899 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	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	947	947
Object	pinkeylen	pinkeylen

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
947.       pinkeycopy = malloc(pinkeylen);
```

Wrong Size t Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=346
Status	New

The function packetlen in curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c at line 247 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	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	269	269
Object	packetlen	packetlen

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_subscribe(struct Curl_easy *data)

```
....
269.     packet = malloc(packetlen);
```

Wrong Size t Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=347

Status	New

The function data_len in curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c at line 1627 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	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	1660	1660
Object	data_len	data_len

Code Snippet
File Name	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1660.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=348
Status	New

The function data_len in curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c at line 1627 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	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	1660	1660
Object	data_len	data_len

Code Snippet
File Name	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1660.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=349
Status	New

The function outlen in curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c at line 808 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	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	821	821
Object	outlen	outlen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
821.    output = malloc(outlen);
```

Wrong Size t Allocation\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=350
Status	New

The function pinkeylen in curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c at line 928 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	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	976	976
Object	pinkeylen	pinkeylen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
976.      pinkeycopy = malloc(pinkeylen);
```

Wrong Size t Allocation\Path 10:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=351
Status	New

The function data_len in curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c at line 1629 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	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	1663	1663
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1663.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=352
Status	New

The function data_len in curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c at line 1629 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	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	1663	1663
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1663.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 12:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=353
Status	New

The function outlen in curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c at line 816 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	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	829	829
Object	outlen	outlen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
829.     output = malloc(outlen);
```

Wrong Size t Allocation\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=354
Status	New

The function pinkeylen in curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c at line 936 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	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	984	984
Object	pinkeylen	pinkeylen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
984.       pinkeycopy = malloc(pinkeylen);
```

Wrong Size t Allocation\Path 14:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=355
Status	New

The function data_len in curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c at line 1638 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	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	1674	1674
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1674.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=356
Status	New

The function data_len in curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c at line 1936 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	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	1972	1972
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_easy *data, int sockindex,

```
....
1972.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=357
Status	New

The function data_len in curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c at line 1962 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	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	1997	1997
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
1997.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=358
Status	New

The function data_len in curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c at line 1952 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	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	1987	1987
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
1987.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=359
Status	New

The function data_len in curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c at line 1994 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	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	2030	2030
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
2030.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=360
Status	New

The function newlen in curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c at line 54 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	curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c	curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c
Line	101	101
Object	newlen	newlen

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c
Method	bool tool_create_output_file(struct OutStruct *outs,

```
....
101.        newname = malloc(newlen);
```

Wrong Size t Allocation\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=361
Status	New

The function data_len in curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c at line 1942 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	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	1978	1978
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
1978.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=362
Status	New

The function data_len in curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c at line 1964 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	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Line	2000	2000
Object	data_len	data_len

Code Snippet

File Name	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method	schannel_send(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
2000.     ptr = (unsigned char *) malloc(data_len);
```

Wrong Size t Allocation\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=363
Status	New

The function len in dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c at line 205 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	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Line	207	207
Object	len	len

Code Snippet
File Name dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Method copy_address(const struct Address *addr) {

```
....
207.      struct Address *new_addr = malloc(len);
```

Wrong Size t Allocation\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=364
Status	New

The function reallocated_length in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c at line 1001 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	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1057	1057
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c

Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1057.                                           reallocated_length);
```

Wrong Size t Allocation\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=365
Status	New

The function reallocated_length in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c at line 1753 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	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1813	1813
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1813.                                             reallocated_length);
```

Wrong Size t Allocation\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=366
Status	New

The function reallocated_length in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c at line 1753 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	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1902	1902
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1902.                                           reallocated_length);
```

Wrong Size t Allocation\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=367
Status	New

The function reallocated_length in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c at line 1001 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	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1057	1057
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1057.                                     reallocated_length);
```

Wrong Size t Allocation\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=368
Status	New

The function reallocated_length in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c at line 1753 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	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1813	1813
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1813.                                               reallocated_length);
```

Wrong Size t Allocation\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=369
Status	New

The function reallocated_length in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c at line 1753 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	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1902	1902
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1902.                                                    reallocated_length);
```

Wrong Size t Allocation\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=370
Status	New

The function reallocated_length in curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c at line 1018 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	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	1074	1074
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1074.                                         reallocated_length);
```

Wrong Size t Allocation\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=371
Status	New

The function reallocated_length in curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c at line 1770 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	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	1830	1830
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1830.                                           reallocated_length);
```

Wrong Size t Allocation\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=372
Status	New

The function reallocated_length in curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c at line 1770 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	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	1919	1919

Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1919.                                       reallocated_length);
```

Wrong Size t Allocation\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=373
Status	New

The function reallocated_length in curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c at line 1018 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	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	1074	1074
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1074.                                  reallocated_length);
```

Wrong Size t Allocation\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=374
Status	New

The function reallocated_length in curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c at line 1770 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	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c

Line	1830	1830
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1830.                                          reallocated_length);
```

Wrong Size t Allocation\Path 34:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=375
Status New

The function reallocated_length in curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c at line 1770 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	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	1919	1919
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1919.                                              reallocated_length);
```

Wrong Size t Allocation\Path 35:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=376
Status New

The function reallocated_length in curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c at line 1016 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	curl@@curl-curl-7_81_0-CVE-2021-	curl@@curl-curl-7_81_0-CVE-2021-

	22890-FP.c	22890-FP.c
Line	1073	1073
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1073.                                        reallocated_length);
```

Wrong Size t Allocation\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=377
Status	New

The function reallocated_length in curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c at line 1773 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	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	1834	1834
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1834.                                          reallocated_length);
```

Wrong Size t Allocation\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=378
Status	New

The function reallocated_length in curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c at line 1773 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	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	1923	1923
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1923.                                             reallocated_length);
```

Wrong Size t Allocation\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=379
Status	New

The function reallocated_length in curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c at line 1016 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	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	1073	1073
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1073.                                       reallocated_length);
```

Wrong Size t Allocation\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=380
Status	New

The function reallocated_length in curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c at line 1773 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	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	1834	1834
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1834.                                        reallocated_length);
```

Wrong Size t Allocation\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=381
Status	New

The function reallocated_length in curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c at line 1773 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	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	1923	1923
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1923.                                            reallocated_length);
```

Wrong Size t Allocation\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=382
Status	New

The function reallocated_length in curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c at line 1028 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	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	1086	1086
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1086.                                         reallocated_length);
```

Wrong Size t Allocation\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=383
Status	New

The function reallocated_length in curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c at line 1784 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	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	1847	1847
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1847.                                           reallocated_length);
```

Wrong Size t Allocation\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=384
Status	New

The function reallocated_length in curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c at line 1784 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	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	1936	1936
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1936.                                               reallocated_length);
```

Wrong Size t Allocation\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=385
Status	New

The function reallocated_length in curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c at line 1326 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	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	1384	1384
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1384.                                         reallocated_length);
```

Wrong Size t Allocation\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=386
Status	New

The function reallocated_length in curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c at line 2082 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	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	2145	2145
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
2145.                                               reallocated_length);
```

Wrong Size t Allocation\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=387
Status	New

The function reallocated_length in curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c at line 2082 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	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	2234	2234
Object	reallocated_length	reallocated_length

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_recv(struct Curl_easy *data, int sockindex,

```
....
2234.                                                   reallocated_length);
```

Wrong Size t Allocation\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=388
Status	New

The function reallocated_length in curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c at line 1342 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	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	1400	1400
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_cfilter *cf, struct Curl_easy *data)

```
....
1400.                                         reallocated_length);
```

Wrong Size t Allocation\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=389
Status	New

The function reallocated_length in curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c at line 2108 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	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	2170	2170
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
2170.                                           reallocated_length);
```

Wrong Size t Allocation\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=390
Status	New

The function reallocated_length in curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c at line 2108 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	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	2259	2259
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_recv(struct Curl_cfilter *cf, struct Curl_easy *data,

```
....
2259.                                              reallocated_length);
```

Wrong Size t Allocation\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=391
Status	New

The function reallocated_length in curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c at line 1349 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	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	1407	1407
Object	reallocated_length	reallocated_length

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_cfilter *cf, struct Curl_easy *data)

```
....
1407.                                        reallocated_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=1000014&projectid=9&pathid=1970
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2792	2802
Object	ubuf	ubuf

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2792.          free(ubuf);
....
2802.          free(ubuf);
```

Double Free\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1971
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	257	257
Object	per	per

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c

Method static struct per_transfer *del_per_transfer(struct per_transfer *per)

```
....
257.     free(per);
```

Double Free\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1972
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	680	678
Object	separator_err	filename

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
680.    free(per->separator_err);
....
678.      free(outs->filename);
```

Double Free\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1973
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	683	678
Object	uploadfile	filename

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
683.    free(per->uploadfile);
....
678.      free(outs->filename);
```

Double Free\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1974
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-	curl@@curl-curl-7_77_0-CVE-2022-

	27778-TP.c	27778-TP.c
Line	681	678
Object	separator	filename

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
681.     free(per->separator);
....
678.       free(outs->filename);
```

Double Free\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1975
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1094	1103
Object	domain	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1094.          free(clist->domain);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1976
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1097	1103

Object	expirestr	co

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....
1097.           free(clist->expirestr);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1977
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1099	1103
Object	maxage	co

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....
1099.           free(clist->maxage);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1978
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1092	1103
Object	name	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1092.          free(clist->name);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1979
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1095	1103
Object	path	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1095.          free(clist->path);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1980
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1096	1103
Object	spath	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1096.          free(clist->spath);
....
1103.          free(co);   /* free the newly allocated memory */
```

Double Free\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1981
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1093	1103
Object	value	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1093.          free(clist->value);
....
1103.          free(co);   /* free the newly allocated memory */
```

Double Free\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1982
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1098	1103
Object	version	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1098.           free(clist->version);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1983
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2792	2802
Object	ubuf	ubuf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2792.         free(ubuf);
....
2802.         free(ubuf);
```

Double Free\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1984
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1094	1103
Object	domain	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1094.           free(clist->domain);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1985
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1097	1103
Object	expirestr	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1097.           free(clist->expirestr);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1986
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1099	1103
Object	maxage	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1099.           free(clist->maxage);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1987
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1092	1103
Object	name	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1092.           free(clist->name);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1988
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1095	1103
Object	path	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1095.           free(clist->path);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1989
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1096	1103
Object	spath	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1096.           free(clist->spath);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1990
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1093	1103
Object	value	co

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1093.           free(clist->value);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1991
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1098	1103
Object	version	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1098.           free(clist->version);
....
1103.           free(co);   /* free the newly allocated memory */
```

Double Free\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1992
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1094	1103
Object	domain	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1094.          free(clist->domain);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1993
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1097	1103
Object	expirestr	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1097.          free(clist->expirestr);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1994
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1099	1103
Object	maxage	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1099.           free(clist->maxage);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1995
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1092	1103
Object	name	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1092.           free(clist->name);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1996
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1095	1103
Object	path	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1095.           free(clist->path);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1997
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1096	1103
Object	spath	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1096.           free(clist->spath);
....
1103.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1998
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1093	1103
Object	value	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1093.          free(clist->value);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=1999
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1098	1103
Object	version	co

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1098.          free(clist->version);
....
1103.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2000
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	256	256
Object	per	per

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static struct per_transfer *del_per_transfer(struct per_transfer *per)

```
....
256.     free(per);
```

Double Free\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2001
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	635	634
Object	this_url	filename

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
635.     free(per->this_url);
....
634.       free(outs->filename);
```

Double Free\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2002
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	638	634
Object	outfile	filename

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
638.     free(per->outfile);
....
634.       free(outs->filename);
```

Double Free\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2003
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	637	634
Object	separator	filename

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
637.     free(per->separator);
....
634.       free(outs->filename);
```

Double Free\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2004
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	639	634
Object	uploadfile	filename

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
639.     free(per->uploadfile);
....
634.       free(outs->filename);
```

Double Free\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2005
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1090	1099
Object	domain	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1090.            free(clist->domain);
....
1099.            free(co);    /* free the newly allocated memory */
```

Double Free\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2006
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1093	1099
Object	expirestr	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1093.          free(clist->expirestr);
....
1099.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2007
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1095	1099
Object	maxage	co

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1095.          free(clist->maxage);
....
1099.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2008
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1088	1099
Object	name	co

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1088.          free(clist->name);
....
1099.          free(co);   /* free the newly allocated memory */
```

Double Free\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2009
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1091	1099
Object	path	co

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1091.          free(clist->path);
....
1099.          free(co);   /* free the newly allocated memory */
```

Double Free\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2010
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1092	1099
Object	spath	co

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1092.           free(clist->spath);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2011
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1089	1099
Object	value	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1089.           free(clist->value);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2012
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1094	1099
Object	version	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1094.          free(clist->version);
....
1099.          free(co);    /* free the newly allocated memory */
```

Double Free\Path 44:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2013
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	2812	2822
Object	ubuf	ubuf

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method	CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2812.        free(ubuf);
....
2822.        free(ubuf);
```

Double Free\Path 45:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2014
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1090	1099
Object	domain	co

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1090.           free(clist->domain);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2015
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1093	1099
Object	expirestr	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1093.           free(clist->expirestr);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 47:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2016
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1095	1099
Object	maxage	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1095.           free(clist->maxage);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 48:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2017
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1088	1099
Object	name	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1088.           free(clist->name);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 49:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2018
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1091	1099
Object	path	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1091.           free(clist->path);
....
1099.           free(co);    /* free the newly allocated memory */
```

Double Free\Path 50:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2019
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1092	1099
Object	spath	co

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1092.           free(clist->spath);
....
1099.           free(co);    /* free the newly allocated memory */
```

Heap Inspection

Query Path:
CPP\Cx\CPP Medium Threat\Heap Inspection Version:1

Categories

OWASP Top 10 2013: A6-Sensitive Data Exposure
FISMA 2014: Media Protection
NIST SP 800-53: SC-4 Information in Shared Resources (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Heap Inspection\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2093
Status	New

Method schannel_connect_step1 at line 418 of curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	659	659
Object	pszPassword	pszPassword

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
659.            WCHAR* pszPassword;
```

Heap Inspection\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2094
Status	New

Method schannel_connect_step1 at line 418 of curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	659	659
Object	pszPassword	pszPassword

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
659.            WCHAR* pszPassword;
```

Heap Inspection\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2095
Status	New

Method schannel_acquire_credential_handle at line 417 of curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	568	568
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
568.        WCHAR* pszPassword;
```

Heap Inspection\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2096
Status	New

Method schannel_acquire_credential_handle at line 417 of curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	568	568
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
568.        WCHAR* pszPassword;
```

Heap Inspection\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2097
Status	New

Method schannel_acquire_credential_handle at line 415 of curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	567	567
Object	pszPassword	pszPassword

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
567.        WCHAR* pszPassword;
```

Heap Inspection\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2098
Status	New

Method schannel_acquire_credential_handle at line 415 of curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	567	567
Object	pszPassword	pszPassword

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
567.        WCHAR* pszPassword;
```

Heap Inspection\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2099
Status	New

Method schannel_acquire_credential_handle at line 417 of curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	572	572
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
572.         WCHAR* pszPassword;
```

Heap Inspection\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2100
Status	New

Method schannel_acquire_credential_handle at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	628	628
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
628.         WCHAR* pszPassword;
```

Heap Inspection\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2101
Status	New

Method parsenetrc at line 58 of curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c defines password, which is designated to contain user passwords. However, while plaintext passwords are later assigned to password, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Line	68	68
Object	password	password

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Method static int parsenetrc(const char *host,

```
....
68.     char *password = *passwordp;
```

Heap Inspection\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2102
Status	New

Method schannel_acquire_credential_handle at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	629	629
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
629.        WCHAR* pszPassword;
```

Heap Inspection\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2103
Status	New

Method schannel_acquire_credential_handle at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	634	634
Object	pszPassword	pszPassword

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
634.         WCHAR* pszPassword;
```

Heap Inspection\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2104
Status	New

Method schannel_acquire_credential_handle at line 484 of curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	634	634
Object	pszPassword	pszPassword

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
634.         WCHAR* pszPassword;
```

Heap Inspection\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2105
Status	New

Method schannel_acquire_credential_handle at line 449 of curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	599	599
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
599.        WCHAR* pszPassword;
```

Heap Inspection\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2106
Status	New

Method schannel_acquire_credential_handle at line 449 of curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c defines pszPassword, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pszPassword, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Line	599	599
Object	pszPassword	pszPassword

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
599.        WCHAR* pszPassword;
```

Heap Inspection\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2107
Status	New

Method http_output_basic at line 299 of curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Line	305	305
Object	pwd	pwd

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27776-TP.c
Method	static CURLcode http_output_basic(struct Curl_easy *data, bool proxy)

```
....
305.     const char *pwd;
```

Heap Inspection\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2108
Status	New

Method http_output_basic at line 299 of curl@@curl-curl-7_79_0-CVE-2022-27776-TP.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27776-TP.c
Line	305	305
Object	pwd	pwd

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27776-TP.c
Method	static CURLcode http_output_basic(struct Curl_easy *data, bool proxy)

```
....
305.     const char *pwd;
```

Heap Inspection\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2109
Status	New

Method http_output_basic at line 299 of curl@@curl-curl-7_81_0-CVE-2022-27776-TP.c defines pwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27776-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27776-TP.c
Line	305	305
Object	pwd	pwd

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27776-TP.c
Method static CURLcode http_output_basic(struct Curl_easy *data, bool proxy)

```
....
305.     const char *pwd;
```

Heap Inspection\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2110
Status	New

Method schannel_connect_step1 at line 418 of curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	660	660
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
660.         size_t pwd_len = 0;
```

Heap Inspection\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2111
Status	New

Method schannel_connect_step1 at line 418 of curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	660	660
Object	pwd_len	pwd_len

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
660.           size_t pwd_len = 0;
```

Heap Inspection\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2112
Status	New

Method schannel_acquire_credential_handle at line 417 of curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	569	569
Object	pwd_len	pwd_len

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
569.         size_t pwd_len = 0;
```

Heap Inspection\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2113
Status	New

Method schannel_acquire_credential_handle at line 417 of curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	569	569
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
569.          size_t pwd_len = 0;
```

Heap Inspection\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2114
Status	New

Method schannel_acquire_credential_handle at line 415 of curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	568	568
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
568.          size_t pwd_len = 0;
```

Heap Inspection\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2115
Status	New

Method schannel_acquire_credential_handle at line 415 of curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	568	568
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
568.        size_t pwd_len = 0;
```

Heap Inspection\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2116
Status	New

Method schannel_acquire_credential_handle at line 417 of curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	573	573
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
573.        size_t pwd_len = 0;
```

Heap Inspection\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2117
Status	New

Method schannel_acquire_credential_handle at line 481 of curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	629	629
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
629.        size_t pwd_len = 0;
```

Heap Inspection\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2118
Status	New

Method schannel_acquire_credential_handle at line 480 of curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	630	630
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
630.        size_t pwd_len = 0;
```

Heap Inspection\Path 27:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2119
Status	New

Method schannel_acquire_credential_handle at line 485 of curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	635	635
Object	pwd_len	pwd_len

Code Snippet

File Name	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
635.          size_t pwd_len = 0;
```

Heap Inspection\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2120
Status	New

Method schannel_acquire_credential_handle at line 484 of curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	635	635
Object	pwd_len	pwd_len

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
635.          size_t pwd_len = 0;
```

Heap Inspection\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2121
Status	New

Method schannel_acquire_credential_handle at line 449 of curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	600	600
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
600.        size_t pwd_len = 0;
```

Heap Inspection\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2122
Status	New

Method schannel_acquire_credential_handle at line 449 of curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c defines pwd_len, which is designated to contain user passwords. However, while plaintext passwords are later assigned to pwd_len, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Line	600	600
Object	pwd_len	pwd_len

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
600.        size_t pwd_len = 0;
```

Heap Inspection\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2123
Status	New

Method imap_perform_login at line 499 of curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c
Line	504	504
Object	passwd	passwd

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
504.    char *passwd;
```

Heap Inspection\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2124
Status	New

Method imap_perform_login at line 501 of curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c
Line	506	506
Object	passwd	passwd

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
506.    char *passwd;
```

Heap Inspection\Path 33:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2125
Status	New

Method imap_perform_login at line 501 of curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c
Line	506	506
Object	passwd	passwd

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
506.     char *passwd;
```

Heap Inspection\Path 34:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2126
Status	New

Method imap_perform_login at line 504 of curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c
Line	509	509
Object	passwd	passwd

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
509.     char *passwd;
```

Heap Inspection\Path 35:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2127
Status	New

Method imap_perform_login at line 505 of curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c
Line	510	510
Object	passwd	passwd

Code Snippet

File Name curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c

Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
510.    char *passwd;
```

Heap Inspection\Path 36:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2128
Status	New

Method imap_perform_login at line 507 of curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c
Line	512	512
Object	passwd	passwd

Code Snippet

File Name curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c

Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
512.    char *passwd;
```

Heap Inspection\Path 37:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2129
Status	New

Method imap_perform_login at line 504 of curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c
Line	509	509
Object	passwd	passwd

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
509.     char *passwd;
```

Heap Inspection\Path 38:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2130
Status	New

Method imap_perform_login at line 505 of curl@@curl-curl-8_6_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22947-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22947-FP.c
Line	510	510
Object	passwd	passwd

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22947-FP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
510.     char *passwd;
```

Heap Inspection\Path 39:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2131
Status	New

Method imap_perform_login at line 507 of curl@@curl-curl-8_8_0-CVE-2021-22947-FP.c defines passwd, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwd, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22947-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22947-FP.c
Line	512	512
Object	passwd	passwd

Code Snippet

File Name	curl@@curl-curl-8_8_0-CVE-2021-22947-FP.c
Method	static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
512.     char *passwd;
```

Heap Inspection\Path 40:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2132
Status	New

Method override_login at line 2866 of curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c defines passwdp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwdp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	2871	2871
Object	passwdp	passwdp

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode override_login(struct Curl_easy *data,

```
....
2871.     char **passwdp = &conn->passwd;
```

Heap Inspection\Path 41:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2133
Status	New

Method override_login at line 2866 of curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c defines passwdp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwdp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	2871	2871
Object	passwdp	passwdp

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static CURLcode override_login(struct Curl_easy *data,

```
....
2871.     char **passwdp = &conn->passwd;
```

Heap Inspection\Path 42:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2134
Status	New

Method override_login at line 2886 of curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c defines passwdp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwdp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	2891	2891
Object	passwdp	passwdp

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method	static CURLcode override_login(struct Curl_easy *data,

```
....
2891.     char **passwdp = &conn->passwd;
```

Heap Inspection\Path 43:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2135
Status	New

Method override_login at line 2916 of curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c defines passwdp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwdp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Line	2921	2921
Object	passwdp	passwdp

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Method static CURLcode override_login(struct Curl_easy *data,

```
....
2921.     char **passwdp = &conn->passwd;
```

Heap Inspection\Path 44:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2136
Status New

Method override_login at line 2913 of curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c defines passwdp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwdp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Line	2918	2918
Object	passwdp	passwdp

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Method static CURLcode override_login(struct Curl_easy *data,

```
....
2918.     char **passwdp = &conn->passwd;
```

Heap Inspection\Path 45:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2137
Status New

Method parsenetrc at line 58 of curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c defines passwordp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwordp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Line	60	60
Object	passwordp	passwordp

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Method static int parsenetrc(const char *host,

```
....
60.                           char **passwordp,
```

Heap Inspection\Path 46:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2138
Status	New

Method Curl_parsenetrc at line 284 of curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c defines passwordp, which is designated to contain user passwords. However, while plaintext passwords are later assigned to passwordp, this variable is never cleared from memory.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Line	286	286
Object	passwordp	passwordp

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Method int Curl_parsenetrc(const char *host,

```
....
286.                          char **passwordp,
```

Divide By Zero

Query Path:
CPP\Cx\CPP Medium Threat\Divide By Zero Version:1

Description

Divide By Zero\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=310
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c. In line 729, the program attempts to divide by nx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input nx in pixBlockconvTiled of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c, at line 729.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	761	761
Object	nx	nx

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
761.        xrat = w / nx;
```

Divide By Zero\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=311
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c. In line 729, the program attempts to divide by ny, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ny in pixBlockconvTiled of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c, at line 729.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	762	762
Object	ny	ny

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
762.        yrat = h / ny;
```

Divide By Zero\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	[pathid=312](http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=312)
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c. In line 729, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c, at line 729.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	764	764
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
764.          nx = w / (wc + 2);
```

Divide By Zero\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=313
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c. In line 729, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c, at line 729.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	768	768
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
768.          ny = h / (hc + 2);
```

Divide By Zero\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=314
Status	New

The application performs an illegal operation in pixWindowedMean, in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c. In line 1067, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMean of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c, at line 1067.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	1125	1125
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method pixWindowedMean(PIX *pixs,

```
....
1125.           norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=315
Status	New

The application performs an illegal operation in pixWindowedMeanSquare, in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c. In line 1184, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMeanSquare of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c, at line 1184.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	1238	1238
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method pixWindowedMeanSquare(PIX *pixs,

```
....
1238.       norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=316
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by nx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input nx in pixBlockconvTiled of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	766	766
Object	nx	nx

Code Snippet

File Name	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method	pixBlockconvTiled(PIX *pix,

```
....
766.       xrat = w / nx;
```

Divide By Zero\Path 8:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=317
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by ny, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ny in pixBlockconvTiled of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	767	767
Object	ny	ny

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
767.      yrat = h / ny;
```

Divide By Zero\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=318
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	769	769
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
769.          nx = w / (wc + 2);
```

Divide By Zero\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=319
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-	DanBloomberg@@leptonica-1.81.0-CVE-

	2022-38266-FP.c	2022-38266-FP.c
Line	773	773
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
773.          ny = h / (hc + 2);
```

Divide By Zero\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=320
Status	New

The application performs an illegal operation in pixWindowedMean, in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c. In line 1073, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMean of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c, at line 1073.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	1131	1131
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method pixWindowedMean(PIX *pixs,

```
....
1131.          norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=321
Status	New

The application performs an illegal operation in pixWindowedMeanSquare, in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c. In line 1190, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMeanSquare of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c, at line 1190.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	1244	1244
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method	pixWindowedMeanSquare(PIX *pixs,

```
....
1244.       norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=322
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by nx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input nx in pixBlockconvTiled of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	766	766
Object	nx	nx

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	pixBlockconvTiled(PIX *pix,

```
....
766.       xrat = w / nx;
```

Divide By Zero\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=323
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by ny, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ny in pixBlockconvTiled of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	767	767
Object	ny	ny

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
767.        yrat = h / ny;
```

Divide By Zero\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=324
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	769	769
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
769.            nx = w / (wc + 2);
```

Divide By Zero\Path 16:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=325
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c. In line 734, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c, at line 734.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	773	773
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	pixBlockconvTiled(PIX *pix,

```
....
773.            ny = h / (hc + 2);
```

Divide By Zero\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=326
Status	New

The application performs an illegal operation in pixWindowedMean, in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c. In line 1073, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMean of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c, at line 1073.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	1131	1131
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	pixWindowedMean(PIX *pixs,

```
....
1131.          norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=327
Status	New

The application performs an illegal operation in pixWindowedMeanSquare, in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c. In line 1190, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMeanSquare of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c, at line 1190.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	1244	1244
Object	BinaryExpr	BinaryExpr

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	pixWindowedMeanSquare(PIX *pixs,

```
....
1244.      norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 19:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=328
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by nx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input nx in pixBlockconvTiled of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	752	752
Object	nx	nx

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
752.       xrat = w / nx;
```

Divide By Zero\Path 20:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=329
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by ny, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ny in pixBlockconvTiled of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	753	753
Object	ny	ny

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
753.       yrat = h / ny;
```

Divide By Zero\Path 21:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=330
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-	DanBloomberg@@leptonica-1.83.0-CVE-

	2022-38266-FP.c	2022-38266-FP.c
Line	755	755
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
755.            nx = w / (wc + 2);
```

Divide By Zero\Path 22:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=331
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	759	759
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
759.            ny = h / (hc + 2);
```

Divide By Zero\Path 23:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=332
Status	New

The application performs an illegal operation in pixWindowedMean, in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c. In line 1055, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMean of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c, at line 1055.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	1111	1111
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method pixWindowedMean(PIX *pixs,

```
....
1111.          norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 24:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=333
Status	New

The application performs an illegal operation in pixWindowedMeanSquare, in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c. In line 1170, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMeanSquare of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c, at line 1170.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	1222	1222
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method pixWindowedMeanSquare(PIX *pixs,

```
....
1222.      norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 25:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=334

Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by nx, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input nx in pixBlockconvTiled of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	752	752
Object	nx	nx

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
752.        xrat = w / nx;
```

Divide By Zero\Path 26:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=335
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by ny, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input ny in pixBlockconvTiled of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	753	753
Object	ny	ny

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
753.        yrat = h / ny;
```

Divide By Zero\Path 27:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=336
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	755	755
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
755.            nx = w / (wc + 2);
```

Divide By Zero\Path 28:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=337
Status	New

The application performs an illegal operation in pixBlockconvTiled, in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c. In line 722, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixBlockconvTiled of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c, at line 722.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	759	759
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method pixBlockconvTiled(PIX *pix,

```
....
759.            ny = h / (hc + 2);
```

Divide By Zero\Path 29:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=338
Status	New

The application performs an illegal operation in pixWindowedMean, in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c. In line 1055, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMean of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c, at line 1055.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	1111	1111
Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method pixWindowedMean(PIX *pixs,

```
....
1111.           norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 30:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=339
Status	New

The application performs an illegal operation in pixWindowedMeanSquare, in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c. In line 1170, the program attempts to divide by BinaryExpr, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input BinaryExpr in pixWindowedMeanSquare of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c, at line 1170.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	1222	1222

Object	BinaryExpr	BinaryExpr

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method pixWindowedMeanSquare(PIX *pixs,

```
....
1222.       norm = 1.0 / ((l_float32)(wincr) * hincr);
```

Divide By Zero\Path 31:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=340
Status	New

The application performs an illegal operation in CJSON_PUBLIC, in DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c. In line 105, the program attempts to divide by 0, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input 0 in CJSON_PUBLIC of DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c, at line 105.

	Source	Destination
File	DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c
Line	109	109
Object	0	0

Code Snippet
File Name DaveGamble@@cJSON-v1.7.13-CVE-2024-31755-TP.c
Method CJSON_PUBLIC(double) cJSON_GetNumberValue(cJSON *item)

```
....
109.          return NAN;
```

Divide By Zero\Path 32:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=341
Status	New

The application performs an illegal operation in CJSON_PUBLIC, in DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c. In line 105, the program attempts to divide by 0, which might be evaluate to 0 (zero) at time of division. This value could be a hard-coded zero value, or received from external, untrusted input 0 in CJSON_PUBLIC of DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c, at line 105.

	Source	Destination

File	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c	DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c
Line	109	109
Object	0	0

Code Snippet
File Name DaveGamble@@cJSON-v1.7.14-CVE-2024-31755-TP.c
Method CJSON_PUBLIC(double) cJSON_GetNumberValue(const cJSON * const item)

```
....
109.            return (double) NAN;
```

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=1000014&projectid=9&pathid=3212
Status	New

	Source	Destination
File	DMTF@@libspdm-2.0.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.0.0-CVE-2023-32690-TP.c
Line	40	51
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.0.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
40.       uint8_t *sender_buffer;
....
51.       message = sender_buffer;
```

Use of Uninitialized Variable\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3213

Status	New

	Source	Destination
File	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Line	40	61
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
40.      uint8_t *sender_buffer;
....
61.           message = sender_buffer;
```

Use of Uninitialized Variable\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3214
Status	New

	Source	Destination
File	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Line	40	59
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
40.      uint8_t *sender_buffer;
....
59.      if ((uint8_t*) request >= sender_buffer &&
```

Use of Uninitialized Variable\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3215
Status	New

	Source	Destination
File	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Line	40	60
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
40.       uint8_t *sender_buffer;
....
60.            (uint8_t*)request < sender_buffer + sender_buffer_size) {
```

Use of Uninitialized Variable\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3216
Status	New

	Source	Destination
File	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Line	252	284
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
252.       uint8_t *scratch_buffer;
....
284.       send_info->large_message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_MESSAGE_OFFSET;
```

Use of Uninitialized Variable\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3217
Status	New

	Source	Destination

File	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Line	252	276
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.1.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
252.      uint8_t *scratch_buffer;
....
276.      message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 7:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3218
Status New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	36	67
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
36.      uint8_t *scratch_buffer;
....
67.              message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 8:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3219
Status New

	Source	Destination

File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	36	74
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
36.       uint8_t *scratch_buffer;
....
74.                message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET;
```

Use of Uninitialized Variable\Path 9:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3220
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	36	70
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
36.       uint8_t *scratch_buffer;
....
70.                       scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 10:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3221
Status	New

	Source	Destination

File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	36	72
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
36.      uint8_t *scratch_buffer;
....
72.                      scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3222
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	36	64
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
36.      uint8_t *scratch_buffer;
....
64.           if ((uint8_t*)request >= scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3223
Status	New

	Source	Destination

File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	36	65
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
36.       uint8_t *scratch_buffer;
....
65.                 && (uint8_t*)request < scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET
```

Use of Uninitialized Variable\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3224
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	39	60
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
39.       uint8_t *sender_buffer;
....
60.           message = sender_buffer;
```

Use of Uninitialized Variable\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3225
Status	New

	Source	Destination

File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	39	58
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
39.       uint8_t *sender_buffer;
....
58.       if ((uint8_t*) request >= sender_buffer &&
```

Use of Uninitialized Variable\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3226
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	39	59
Object	sender_buffer	sender_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_send_request(void *context, const uint32_t *session_id,

```
....
39.       uint8_t *sender_buffer;
....
59.           (uint8_t*)request < sender_buffer + sender_buffer_size) {
```

Use of Uninitialized Variable\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3227
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-	DMTF@@libspdm-2.2.0-CVE-2023-

	32690-TP.c	32690-TP.c
Line	157	190
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_receive_response(void *context, const uint32_t *session_id,

```
....
157.      uint8_t *scratch_buffer;
....
190.      *response = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SECURE_MESSAGE_OFFSET +
```

Use of Uninitialized Variable\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3228
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c	DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Line	270	300
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
270.      uint8_t *scratch_buffer;
....
300.      send_info->large_message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_LARGE_MESSAGE_OFFSET;
```

Use of Uninitialized Variable\Path 18:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3229
Status	New

	Source	Destination
File	DMTF@@libspdm-2.2.0-CVE-2023-	DMTF@@libspdm-2.2.0-CVE-2023-

	32690-TP.c	32690-TP.c
Line	270	292
Object	scratch_buffer	scratch_buffer

Code Snippet
File Name DMTF@@libspdm-2.2.0-CVE-2023-32690-TP.c
Method libspdm_return_t libspdm_handle_large_request(

```
....
270.        uint8_t *scratch_buffer;
....
292.        message = scratch_buffer +
LIBSPDM_SCRATCH_BUFFER_SENDER_RECEIVER_OFFSET;
```

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=1000014&projectid=9&pathid=538
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 868 of curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Line	939	939
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
939.          port = (int)tmp_port;
```

Integer Overflow\Path 2:

Severity	Medium

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=539
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2989 of curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3067	3067
Object	AssignExpr	AssignExpr

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3067.          port = (int)portparse; /* we know it will fit */
```

Integer Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=540
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2989 of curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3067	3067
Object	AssignExpr	AssignExpr

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3067.          port = (int)portparse; /* we know it will fit */
```

Integer Overflow\Path 4:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=541
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 881 of curl@@curl-curl-7_77_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_77_0-CVE-2023-28320-TP.c
Line	952	952
Object	AssignExpr	AssignExpr

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2023-28320-TP.c

Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
952.        port = (int)tmp_port;
```

Integer Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=542
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3013 of curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	3092	3092
Object	AssignExpr	AssignExpr

Code Snippet

File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c

Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3092.         port = (int)portparse; /* we know it will fit */
```

Integer Overflow\Path 6:

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

	[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=543]()
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1008 of curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c
Line	1079	1079
Object	AssignExpr	AssignExpr

Code Snippet

File Name curl@@curl-curl-7_79_0-CVE-2023-28320-TP.c

Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
1079.         port = (int)tmp_port;
```

Integer Overflow\Path 7:

Severity	Medium
Result State	To Verify
Online Results	[http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=544]()
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3043 of curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Line	3122	3122
Object	AssignExpr	AssignExpr

Code Snippet

File Name curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c

Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3122.          port = (int)portparse; /* we know it will fit */
```

Integer Overflow\Path 8:

Severity	Medium
Result State	To Verify
Online Results	[http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&]()

pathid=545
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1020 of curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c
Line	1091	1091
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
1091.         port = (int)tmp_port;
```

Integer Overflow\Path 9:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=546
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3056 of curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Line	3135	3135
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3135.          port = (int)portparse; /* we know it will fit */
```

Integer Overflow\Path 10:

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=547

Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1020 of curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c
Line	1091	1091
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
1091.          port = (int)tmp_port;
```

Integer Overflow\Path 11:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=548
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1034 of curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c
Line	1105	1105
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
1105.          port = (int)tmp_port;
```

Integer Overflow\Path 12:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=549
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1116 of curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Line	1181	1181
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_wait(struct Curl_multi *multi,

```
....
1181.       timeout_ms = (int)timeout_internal;
```

Integer Overflow\Path 13:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=550
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1059 of curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c	curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c
Line	1130	1130
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
1130.         port = (int)tmp_port;
```

Integer Overflow\Path 14:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=551
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1149 of curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Line	1214	1214
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_wait(struct Curl_multi *multi,

```
....
1214.       timeout_ms = (int)timeout_internal;
```

Integer Overflow\Path 15:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=552
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1162 of curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c
Line	1217	1217
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_wait(struct Curl_multi *multi,

```
....
1217.       timeout_ms = (int)timeout_internal;
```

Integer Overflow\Path 16:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=553
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1214 of curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c
Line	1261	1261
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_wait(struct Curl_multi *multi,

```
....
1261.       timeout_ms = (int)timeout_internal;
```

Integer Overflow\Path 17:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=554
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1319 of curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c
Line	1359	1359
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_wait(struct Curl_multi *multi,

```
....
1359.       timeout_ms = (int)timeout_internal;
```

Wrong Memory Allocation

Query Path:
CPP\Cx\CPP Medium Threat\Wrong Memory Allocation Version:0

Categories

NIST SP 800-53: SI-10 Information Input Validation (P1)

Description

Wrong Memory Allocation\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3872
Status	New

The function malloc in DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c at line 558 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	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c
Line	569	569
Object	sizeof	malloc

Code Snippet

File Name	DarkFlippers@@unleashed-firmware-un1-9b1384-CVE-2022-40363-TP.c
Method	bool nfc_device_load_mifare_df_data(FlipperFormat* file, NfcDevice* dev) {

```
....
569.                data->free_memory =
malloc(sizeof(MifareDesfireFreeMemory));
```

Wrong Memory Allocation\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3873
Status	New

The function malloc in davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c at line 878 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	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c
Line	882	882
Object	sizeof	malloc

Code Snippet

File Name	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c
Method	_dwarf_get_debug(void)

```
....
882.        dbg = (Dwarf_Debug) malloc(sizeof(struct Dwarf_Debug_s));
```

Wrong Memory Allocation\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3874
Status	New

The function malloc in davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c at line 878 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	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c
Line	882	882
Object	sizeof	malloc

Code Snippet

File Name	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c
Method	_dwarf_get_debug(void)

```
....
882.        dbg = (Dwarf_Debug) malloc(sizeof(struct Dwarf_Debug_s));
```

Wrong Memory Allocation\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3875
Status	New

The function malloc in davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c at line 875 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	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c
Line	879	879
Object	sizeof	malloc

Code Snippet

File Name	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c
Method	_dwarf_get_debug(void)

```
....
879.      dbg = (Dwarf_Debug) malloc(sizeof(struct Dwarf_Debug_s));
```

Wrong Memory Allocation\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3876
Status	New

The function malloc in davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c at line 875 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	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c
Line	879	879
Object	sizeof	malloc

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c
Method _dwarf_get_debug(void)

```
....
879.      dbg = (Dwarf_Debug) malloc(sizeof(struct Dwarf_Debug_s));
```

Wrong Memory Allocation\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3877
Status	New

The function malloc in davea42@@libdwarf-code-v0.8.0-CVE-2024-2002-TP.c at line 992 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	davea42@@libdwarf-code-v0.8.0-CVE-2024-2002-TP.c	davea42@@libdwarf-code-v0.8.0-CVE-2024-2002-TP.c
Line	996	996
Object	sizeof	malloc

Code Snippet
File Name davea42@@libdwarf-code-v0.8.0-CVE-2024-2002-TP.c

Method	_dwarf_get_debug(Dwarf_Unsigned filesize)

```
....
996.        dbg = (Dwarf_Debug) malloc(sizeof(struct Dwarf_Debug_s));
```

Wrong Memory Allocation\Path 7:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3878
Status	New

The function malloc in davea42@@libdwarf-code-v0.8.0-CVE-2024-31745-TP.c at line 992 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	davea42@@libdwarf-code-v0.8.0-CVE-2024-31745-TP.c	davea42@@libdwarf-code-v0.8.0-CVE-2024-31745-TP.c
Line	996	996
Object	sizeof	malloc

Code Snippet

File Name	davea42@@libdwarf-code-v0.8.0-CVE-2024-31745-TP.c
Method	_dwarf_get_debug(Dwarf_Unsigned filesize)

```
....
996.        dbg = (Dwarf_Debug) malloc(sizeof(struct Dwarf_Debug_s));
```

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=1000014&projectid=9&pathid=532
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 146 of curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	163	163
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_connect(struct Curl_easy *data)

```
....
163.     packet[1] = (packetlen - 2) & 0x7f;
```

Char Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=533
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 231 of curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Line	237	237
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22945-TP.c
Method static int mqtt_encode_len(char *buf, size_t len)

```
....
237.       encoded = len % 0x80;
```

Char Overflow\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=534
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 141 of davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c
Line	144	144
Object	AssignExpr	AssignExpr

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-2002-TP.c
Method int dwarf_set_de_alloc_flag(int v)

```
....
144.        global_de_alloc_tree_on = v;
```

Char Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=535
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 141 of davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c	davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c
Line	144	144
Object	AssignExpr	AssignExpr

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.1.1-CVE-2024-31745-FP.c
Method int dwarf_set_de_alloc_flag(int v)

```
....
144.        global_de_alloc_tree_on = v;
```

Char Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=536
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 141 of davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination

File	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c
Line	144	144
Object	AssignExpr	AssignExpr

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-2002-TP.c
Method int dwarf_set_de_alloc_flag(int v)

```
....
144.        global_de_alloc_tree_on = v;
```

Char Overflow\Path 6:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=537
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 141 of davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c	davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c
Line	144	144
Object	AssignExpr	AssignExpr

Code Snippet
File Name davea42@@libdwarf-code-libdwarf-0.3.1-CVE-2024-31745-FP.c
Method int dwarf_set_de_alloc_flag(int v)

```
....
144.        global_de_alloc_tree_on = v;
```

Boolean Overflow

Query Path:
CPP\Cx\CPP Integer Overflow\Boolean 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

Boolean Overflow\Path 1:

Severity	Medium
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=527
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 976 of curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	998	998
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
998.         dead = (state & CONNRESULT_DEAD);
```

Boolean Overflow\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=528
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 976 of curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	998	998
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
998.         dead = (state & CONNRESULT_DEAD);
```

Boolean Overflow\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=529
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 992 of curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	1014	1014
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
1014.         dead = (state & CONNRESULT_DEAD);
```

Boolean Overflow\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=530
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1017 of curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Line	1039	1039
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
1039.         dead = (state & CONNRESULT_DEAD);
```

Boolean Overflow\Path 5:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=531
Status	New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1004 of curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c. This will cause a loss of data, often the significant bits of a numerical value or the sign bit.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Line	1026	1026
Object	AssignExpr	AssignExpr

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
1026.         dead = (state & CONNRESULT_DEAD);
```

Inadequate Encryption Strength

Query Path:
CPP\Cx\CPP Medium Threat\Inadequate Encryption Strength Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: SC-13 Cryptographic Protection (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Inadequate Encryption Strength\Path 1:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2139
Status	New

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 424 of curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c at line 424.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Line	451	450
Object	passwd	Curl_MD5_update

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct Curl_easy *data,

```
....
451.                    curlx_uztoui(strlen(conn->passwd)));
....
450.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

Inadequate Encryption Strength\Path 2:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2140
Status	New

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 424 of curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c at line 424.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Line	450	450
Object	passwd	Curl_MD5_update

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct Curl_easy *data,

```
....
450.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

Inadequate Encryption Strength\Path 3:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2141
Status	New

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 424 of curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c at line 424.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c
Line	451	450
Object	passwd	Curl_MD5_update

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c

Method static CURLcode pop3_perform_apop(struct Curl_easy *data,

```
....
451.                    curlx_uztoui(strlen(conn->passwd)));
....
450.     Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

Inadequate Encryption Strength\Path 4:

Severity	Medium
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=2142
Status	New

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 424 of curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c at line 424.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c
Line	450	450
Object	passwd	Curl_MD5_update

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct Curl_easy *data,

```
....
450.     Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

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=1000014&projectid=9&pathid=4159
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1001 of curl@@curl-curl-7_77_0-CVE-2021-22890-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	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1103	1103
Object	malloc	malloc

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1103.      InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(BACKEND-
>encdata_offset),
```

Unchecked Return Value\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4160
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1001 of curl@@curl-curl-7_77_0-CVE-2021-22901-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	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1103	1103
Object	malloc	malloc

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1103.      InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(BACKEND-
>encdata_offset),
```

Unchecked Return Value\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4161
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	285	285
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
285.        return strdup("SSLv2");
```

Unchecked Return Value\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4162
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	287	287
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
287.        return strdup("SSLv3");
```

Unchecked Return Value\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4163
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	289	289
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
289.      return strdup("TLSv1.0");
```

Unchecked Return Value\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4164
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	292	292
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
292.      return strdup("TLSv1.1");
```

Unchecked Return Value\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4165

Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	296	296
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
296.      return strdup("TLSv1.2");
```

Unchecked Return Value\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4166
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	300	300
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
300.      return strdup("TLSv1.3");
```

Unchecked Return Value\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=4167
Status	New

The *dup_nickname method calls the strdup function, at line 424 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	430	430
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
430.       return strdup(str);
```

Unchecked Return Value\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4168
Status	New

The *dup_nickname method calls the strdup function, at line 424 of curl@@curl-curl-7_77_0-CVE-2022-27781-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	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	437	437
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method	static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
437.       return strdup(str);
```

Unchecked Return Value\Path 11:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4169
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1018 of curl@@curl-curl-7_79_0-CVE-2021-22890-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	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	1120	1120
Object	malloc	malloc

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1120.       InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(BACKEND-
>encdata_offset),
```

Unchecked Return Value\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4170
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1018 of curl@@curl-curl-7_79_0-CVE-2021-22901-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	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	1120	1120
Object	malloc	malloc

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1120.       InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(BACKEND-
>encdata_offset),
```

Unchecked Return Value\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4171
Status	New

The *imap_atom method calls the strdup function, at line 1787 of curl@@curl-curl-7_79_0-CVE-2021-22947-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	curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c
Line	1826	1826
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22947-FP.c
Method static char *imap_atom(const char *str, bool escape_only)

```
....
1826.       return strdup(str);
```

Unchecked Return Value\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4172
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	285	285
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
285.       return strdup("SSLv2");
```

Unchecked Return Value\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4173
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	287	287
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
287.        return strdup("SSLv3");
```

Unchecked Return Value\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4174
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	289	289
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
289.        return strdup("TLSv1.0");
```

Unchecked Return Value\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4175
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	292	292
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
292.        return strdup("TLSv1.1");
```

Unchecked Return Value\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4176
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	296	296
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
296.      return strdup("TLSv1.2");
```

Unchecked Return Value\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4177
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	300	300
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
300.      return strdup("TLSv1.3");
```

Unchecked Return Value\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4178
Status	New

The *dup_nickname method calls the strdup function, at line 424 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	430	430
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c

Method	static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
430.        return strdup(str);
```

Unchecked Return Value\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4179
Status	New

The *dup_nickname method calls the strdup function, at line 424 of curl@@curl-curl-7_79_0-CVE-2022-27781-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	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	437	437
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method	static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
437.        return strdup(str);
```

Unchecked Return Value\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4180
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1016 of curl@@curl-curl-7_81_0-CVE-2021-22890-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	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	1119	1119
Object	malloc	malloc

Code Snippet

File Name curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1119.       InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4181
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1016 of curl@@curl-curl-7_81_0-CVE-2021-22901-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	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	1119	1119
Object	malloc	malloc

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1119.       InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4182
Status	New

The *imap_atom method calls the strdup function, at line 1800 of curl@@curl-curl-7_81_0-CVE-2021-22947-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	curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c
Line	1839	1839

Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22947-FP.c
Method	static char *imap_atom(const char *str, bool escape_only)

```
....
1839.       return strdup(str);
```

Unchecked Return Value\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4183
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	285	285
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
285.      return strdup("SSLv2");
```

Unchecked Return Value\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4184
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c

Line	287	287
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
287.        return strdup("SSLv3");
```

Unchecked Return Value\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4185
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	289	289
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
289.        return strdup("TLSv1.0");
```

Unchecked Return Value\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4186
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-	curl@@curl-curl-7_81_0-CVE-2022-

	27781-TP.c	27781-TP.c
Line	292	292
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
292.        return strdup("TLSv1.1");
```

Unchecked Return Value\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4187
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	296	296
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
296.        return strdup("TLSv1.2");
```

Unchecked Return Value\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4188
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	300	300
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
300.        return strdup("TLSv1.3");
```

Unchecked Return Value\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4189
Status	New

The *dup_nickname method calls the strdup function, at line 426 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	432	432
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
432.        return strdup(str);
```

Unchecked Return Value\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4190
Status	New

The *dup_nickname method calls the strdup function, at line 426 of curl@@curl-curl-7_81_0-CVE-2022-27781-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	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	439	439
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method	static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
439.      return strdup(str);
```

Unchecked Return Value\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4191
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1028 of curl@@curl-curl-7_83_0-CVE-2021-22890-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	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	1131	1131
Object	malloc	malloc

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1131.      InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4192
Status	New

The *imap_atom method calls the strdup function, at line 1800 of curl@@curl-curl-7_83_0-CVE-2021-22947-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	curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c
Line	1839	1839
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2021-22947-FP.c
Method	static char *imap_atom(const char *str, bool escape_only)

```
....
1839.       return strdup(str);
```

Unchecked Return Value\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4193
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	285	285
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
285.       return strdup("SSLv2");
```

Unchecked Return Value\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4194
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	287	287
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
287.       return strdup("SSLv3");
```

Unchecked Return Value\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4195
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	289	289
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
289.       return strdup("TLSv1.0");
```

Unchecked Return Value\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4196

Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	292	292
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
292.      return strdup("TLSv1.1");
```

Unchecked Return Value\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4197
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	296	296
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	static char *nss_sslver_to_name(PRUint16 nssver)

```
....
296.      return strdup("TLSv1.2");
```

Unchecked Return Value\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=4198
Status	New

The *nss_sslver_to_name method calls the strdup function, at line 281 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	300	300
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
300.        return strdup("TLSv1.3");
```

Unchecked Return Value\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4199
Status	New

The *dup_nickname method calls the strdup function, at line 426 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	432	432
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
432.        return strdup(str);
```

Unchecked Return Value\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4200
Status	New

The *dup_nickname method calls the strdup function, at line 426 of curl@@curl-curl-7_83_0-CVE-2022-27781-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	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	439	439
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	static char *dup_nickname(struct Curl_easy *data, const char *str)

```
....
439.        return strdup(str);
```

Unchecked Return Value\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4201
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1326 of curl@@curl-curl-7_85_0-CVE-2021-22890-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	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	1429	1429
Object	malloc	malloc

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1429.        InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 44:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4202
Status	New

The *imap_atom method calls the strdup function, at line 1803 of curl@@curl-curl-7_85_0-CVE-2021-22947-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	curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c
Line	1842	1842
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22947-FP.c
Method	static char *imap_atom(const char *str, bool escape_only)

```
....
1842.       return strdup(str);
```

Unchecked Return Value\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4203
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1342 of curl@@curl-curl-7_87_0-CVE-2021-22890-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	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	1445	1445
Object	malloc	malloc

Code Snippet

File Name	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method	schannel_connect_step2(struct Curl_cfilter *cf, struct Curl_easy *data)

```
....
1445.       InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4204
Status	New

The *imap_atom method calls the strdup function, at line 1803 of curl@@curl-curl-7_87_0-CVE-2021-22947-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	curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c
Line	1842	1842
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22947-FP.c
Method static char *imap_atom(const char *str, bool escape_only)

```
....
1842.       return strdup(str);
```

Unchecked Return Value\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4205
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1349 of curl@@curl-curl-8_1_0-CVE-2021-22890-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	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	1452	1452
Object	malloc	malloc

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_connect_step2(struct Curl_cfilter *cf, struct Curl_easy *data)

```
....
1452.       InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4206
Status	New

The *imap_atom method calls the strdup function, at line 1807 of curl@@curl-curl-8_1_0-CVE-2021-22947-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	curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c
Line	1846	1846
Object	strdup	strdup

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22947-FP.c
Method static char *imap_atom(const char *str, bool escape_only)

```
....
1846.       return strdup(str);
```

Unchecked Return Value\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4207
Status	New

The schannel_connect_step2 method calls the malloc function, at line 1366 of curl@@curl-curl-8_3_0-CVE-2021-22890-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	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	1470	1470
Object	malloc	malloc

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method	schannel_connect_step2(struct Curl_cfilter *cf, struct Curl_easy *data)

```
....
1470.      InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(backend-
>encdata_offset),
```

Unchecked Return Value\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4208
Status	New

The *imap_atom method calls the strdup function, at line 1816 of curl@@curl-curl-8_3_0-CVE-2021-22947-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	curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c
Line	1829	1829
Object	strdup	strdup

Code Snippet

File Name	curl@@curl-curl-8_3_0-CVE-2021-22947-FP.c
Method	static char *imap_atom(const char *str, bool escape_only)

```
....
1829.      return strdup(str);
```

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=1000014&projectid=9&pathid=3879
Status	New

	Source	Destination

File	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Line	87	87
Object	fgets	fgets

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Method static int parsenetrc(const char *host,

```
....
87.       while(!done && fgets(netrcbuffer, netrcbuffsize, file)) {
```

Improper Resource Access Authorization\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3880
Status	New

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Line	87	87
Object	netrcbuffer	netrcbuffer

Code Snippet
File Name curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Method static int parsenetrc(const char *host,

```
....
87.       while(!done && fgets(netrcbuffer, netrcbuffsize, file)) {
```

Improper Resource Access Authorization\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3881
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	679	679
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
679.                ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3882
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	679	679
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
679.                ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3883
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	1020	1020
Object	buf	buf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1020.       if((int) fread(buf, size, 1, fp) != 1)
```

Improper Resource Access Authorization\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3884
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	176	176
Object	buffer	buffer

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
176.        ret_stat = fread(buffer, 1, sizeof(buffer), file);
```

Improper Resource Access Authorization\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3885
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1615	1615
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1615.                   ((int)fread(certdata, (size_t)filesize, 1, 
fInCert) != 1))
```

Improper Resource Access Authorization\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=3886
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1658	1658
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1658.              ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3887
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	588	588
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
588.             ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3888
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-	curl@@curl-curl-7_79_0-CVE-2021-

	22901-FP.c	22901-FP.c
Line	588	588
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
588.             ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3889
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	1049	1049
Object	buf	buf

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1049.       if((int) fread(buf, size, 1, fp) != 1)
```

Improper Resource Access Authorization\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3890
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	175	175
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static curl_off_t vms_realfilesize(const char *name,

```
....
175.        ret_stat = fread(buffer, 1, sizeof(buffer), file);
```

Improper Resource Access Authorization\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3891
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	1526	1526
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1526.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3892
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	1569	1569
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1569.              ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3893
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	587	587
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
587.              ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3894
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	587	587
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
587.              ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3895
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	1057	1057
Object	buf	buf

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1057.       if((int) fread(buf, size, 1, fp) != 1)
```

Improper Resource Access Authorization\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3896
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	175	175
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method	static curl_off_t vms_realfilesize(const char *name,

```
....
175.       ret_stat = fread(buffer, 1, sizeof(buffer), file);
```

Improper Resource Access Authorization\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3897
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	1587	1587
Object	certdata	certdata

Code Snippet

File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c

Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1587.                ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3898
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	1630	1630
Object	certdata	certdata

Code Snippet

File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c

Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1630.                ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3899
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c

Line	592	592
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
592.            ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3900
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Line	173	173
Object	buffer	buffer

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Method	static curl_off_t vms_realfilesize(const char *name,

```
....
173.      ret_stat = fread(buffer, 1, sizeof(buffer), file);
```

Improper Resource Access Authorization\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3901
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Line	1585	1585
Object	certdata	certdata

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c

Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1585.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3902
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Line	1628	1628
Object	certdata	certdata

Code Snippet	
File Name	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1628.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

Improper Resource Access Authorization\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3903
Status	New

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	648	648
Object	certdata	certdata

Code Snippet	
File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
648.              ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3904
Status	New

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	649	649
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
649.            ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3905
Status	New

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	654	654
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
654.            ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3906

Status	New

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	654	654
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
654.            ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3907
Status	New

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	619	619
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
619.            ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3908
Status	New

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c

Line	619	619
Object	certdata	certdata

Code Snippet
File Name curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
619.            ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

Improper Resource Access Authorization\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3909
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1579	1579
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1579.         fprintf(out, "#\n# Fatal libcurl error\n");
```

Improper Resource Access Authorization\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3910
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1583	1583
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c

Method	static int cookie_output(struct Curl_easy *data,

```
....
1583.         fprintf(out, "%s\n", format_ptr);
```

Improper Resource Access Authorization\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3911
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	647	647
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_open(struct Curl_easy **curl)

```
....
647.        DEBUGF(fprintf(stderr, "Error: calloc of Curl_easy 
failed\n"));
```

Improper Resource Access Authorization\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3912
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	655	655
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_open(struct Curl_easy **curl)

```
....
655.        DEBUGF(fprintf(stderr, "Error: resolver_init failed\n"));
```

Improper Resource Access Authorization\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3913
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	270	270
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode pre_transfer(struct GlobalConfig *global,

```
....
270.        fprintf(global->errors, "%s\n", per->separator_err);
```

Improper Resource Access Authorization\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3914
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	367	367
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
367.          fprintf(global->errors, "curl: (%d) %s\n", result,
```

Improper Resource Access Authorization\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3915
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	379	379
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
379.            fprintf(global->errors,
```

Improper Resource Access Authorization\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3916
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	412	412
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
412.          fprintf(global->errors, "curl: (%d) Failed writing
body\n", result);
```

Improper Resource Access Authorization\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3917
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c

Line	418	418
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
418.        fprintf(global->errors, "Metalink: fetching (%s) from (%s) 
OK\n",
```

Improper Resource Access Authorization\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3918
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	424	424
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
424.          fprintf(config->global->errors, "Metalink: parsing (%s) 
OK\n",
```

Improper Resource Access Authorization\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3919
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	428	428
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
428.        fprintf(config->global->errors, "Metalink: parsing (%s)
FAILED\n",
```

Improper Resource Access Authorization\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3920
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	576	576
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
576.              fprintf(global->errors,
```

Improper Resource Access Authorization\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3921
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	592	592
Object	fprintf	fprintf

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
592.              fprintf(global->errors,
```

Improper Resource Access Authorization\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3922
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	618	618
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
618.            fprintf(global->errors,
```

Improper Resource Access Authorization\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3923
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	627	627
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
627.        fprintf(global->errors,
```

Improper Resource Access Authorization\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3924

Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	647	647
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
647.          fprintf(global->errors, "curl: (%d) Failed writing
body\n", result);
```

Improper Resource Access Authorization\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3925
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	2146	2146
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
2146.           fprintf(global->errors,
```

Improper Resource Access Authorization\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3926
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c

Line	2150	2150
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
2150.             fprintf(global->errors,
```

Improper Resource Access Authorization\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3927
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1646	1646
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.         fprintf(out, "%s\n", format_ptr);
```

Improper Resource Access Authorization\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3928
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	647	647
Object	fprintf	fprintf

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method CURLcode Curl_open(struct Curl_easy **curl)

```
....
647.       DEBUGF(fprintf(stderr, "Error: calloc of Curl_easy
failed\n"));
```

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=1000014&projectid=9&pathid=4446
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418 is not initialized when it is used by cred at curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	433	512
Object	null	cred

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
433.    struct Curl_schannel_cred *old_cred = NULL;
....
512.                        BACKEND->cred->refcount));
```

NULL Pointer Dereference\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4447
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418 is not initialized when it is used by cred at curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c in line 418.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	433	512
Object	null	cred

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c

Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
433.      struct Curl_schannel_cred *old_cred = NULL;
....
512.                       BACKEND->cred->refcount));
```

NULL Pointer Dereference\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4448
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3474
Object	null	hostname_resolve

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3474.     Curl_safefree(conn->hostname_resolve);
```

NULL Pointer Dereference\Path 4:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4449
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3448
Object	null	socks_proxy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3448.      Curl_safefree(conn->socks_proxy.passwd);
```

NULL Pointer Dereference\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4450
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3446
Object	null	socks_proxy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3446.      Curl_safefree(conn->socks_proxy.user);
```

NULL Pointer Dereference\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4451
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by passwd at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3434
Object	null	passwd

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3434.      Curl_safefree(conn->passwd);
```

NULL Pointer Dereference\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4452
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by user at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3433
Object	null	user

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3433.      Curl_safefree(conn->user);
```

NULL Pointer Dereference\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4453
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3469
Object	null	conn_to_host

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3469.    Curl_safefree(conn->conn_to_host.rawalloc);
```

NULL Pointer Dereference\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4454
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3467
Object	null	conn_to_host

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3467.    Curl_free_idnconverted_hostname(&conn->conn_to_host);
```

NULL Pointer Dereference\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4455
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by encalloc at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 1621.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	1625
Object	null	encalloc

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1625.       idn2_free(host->encalloc); /* must be freed with idn2_free()
since this was
```

NULL Pointer Dereference\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4456
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by encalloc at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 1621.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	1624
Object	null	encalloc

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method	void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1624.     if(host->encalloc) {
```

NULL Pointer Dereference\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4457
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by http_proxy at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3447
Object	null	http_proxy

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

▼

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3447.       Curl_safefree(conn->http_proxy.passwd);
```

NULL Pointer Dereference\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4458
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by http_proxy at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-	curl@@curl-curl-7_77_0-CVE-2022-

	22576-TP.c	22576-TP.c
Line	3523	3445
Object	null	http_proxy

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method	static void reuse_conn(struct Curl_easy *data,

```
....
3445.       Curl_safefree(conn->http_proxy.user);
```

NULL Pointer Dereference\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4459
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by handler at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 4106.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	4120
Object	null	handler

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method	CURLcode Curl_init_do(struct Curl_easy *data, struct connectdata *conn)

```
....
4120.          !(conn->handler->flags & PROTOPT_WILDCARD))
```

NULL Pointer Dereference\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4460
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by bits at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3443
Object	null	bits

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3443.     if(conn->bits.proxy_user_passwd) {
```

NULL Pointer Dereference\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4461
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by bits at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Line	3523	3431
Object	null	bits

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3431.     if(conn->bits.user_passwd) {
```

NULL Pointer Dereference\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4462
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by host at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3468
Object	null	host

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3468.     Curl_safefree(conn->host.rawalloc);
```

NULL Pointer Dereference\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4463
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3517 is not initialized when it is used by host at curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c
Line	3523	3466
Object	null	host

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3466.     Curl_free_idnconverted_hostname(&conn->host);
```

NULL Pointer Dereference\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4464
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c in line 1789 is not initialized when it is used by state at curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c in line 1789.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Line	1793	1814
Object	null	state

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Method	CURLcode Curl_retry_request(struct Curl_easy *data, char **url)

```
....
1793.     *url = NULL;
....
1814.     else if(data->state.refused_stream &&
```

NULL Pointer Dereference\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4465
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 481 is not initialized when it is used by num_connections at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 87.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Line	492	96
Object	null	num_connections

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Method	Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
492.     struct connectbundle *bundle_candidate = NULL;
```

▼

File Name	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Method	static int bundle_remove_conn(struct connectbundle *bundle,

```
....
96.         bundle->num_connections--;
```

NULL Pointer Dereference\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4466
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 481 is not initialized when it is used by conn_list at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 87.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Line	492	95
Object	null	conn_list

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
492.     struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Method static int bundle_remove_conn(struct connectbundle *bundle,

```
....
95.         Curl_llist_remove(&bundle->conn_list, curr, NULL);
```

NULL Pointer Dereference\Path 22:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4467
Status New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 481 is not initialized when it is used by conn_list at curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c in line 87.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Line	492	92
Object	null	conn_list

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
492.     struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27775-TP.c
Method static int bundle_remove_conn(struct connectbundle *bundle,

```
....
92.     curr = bundle->conn_list.head;
```

NULL Pointer Dereference\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4468
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3474
Object	null	hostname_resolve

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3474.     Curl_safefree(conn->hostname_resolve);
```

NULL Pointer Dereference\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4469
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Line	3523	3448
Object	null	socks_proxy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

▼

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3448.       Curl_safefree(conn->socks_proxy.passwd);
```

NULL Pointer Dereference\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4470
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3446
Object	null	socks_proxy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

▼

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3446.       Curl_safefree(conn->socks_proxy.user);
```

NULL Pointer Dereference\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4471
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by passwd at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3434
Object	null	passwd

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

▼

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3434.       Curl_safefree(conn->passwd);
```

NULL Pointer Dereference\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4472
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by user at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3433
Object	null	user

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

▼

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3433.      Curl_safefree(conn->user);
```

NULL Pointer Dereference\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4473
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3469
Object	null	conn_to_host

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

▼

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3469.    Curl_safefree(conn->conn_to_host.rawalloc);
```

NULL Pointer Dereference\Path 29:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4474
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3467
Object	null	conn_to_host

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3467.     Curl_free_idnconverted_hostname(&conn->conn_to_host);
```

NULL Pointer Dereference\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4475
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by encalloc at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 1621.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	1625
Object	null	encalloc

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1625.      idn2_free(host->encalloc); /* must be freed with idn2_free()
since this was
```

NULL Pointer Dereference\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4476
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by encalloc at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 1621.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	1624
Object	null	encalloc

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1624.    if(host->encalloc) {
```

NULL Pointer Dereference\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4477

Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by http_proxy at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3447
Object	null	http_proxy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3447.      Curl_safefree(conn->http_proxy.passwd);
```

NULL Pointer Dereference\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4478
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by http_proxy at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3445
Object	null	http_proxy

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.    struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3445.       Curl_safefree(conn->http_proxy.user);
```

NULL Pointer Dereference\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4479
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by handler at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 4106.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	4120
Object	null	handler

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	CURLcode Curl_init_do(struct Curl_easy *data, struct connectdata *conn)

```
....
4120.          !(conn->handler->flags & PROTOPT_WILDCARD))
```

NULL Pointer Dereference\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4480
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by bits at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3443
Object	null	bits

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3443.     if(conn->bits.proxy_user_passwd) {
```

NULL Pointer Dereference\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4481
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by bits at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3431
Object	null	bits

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3431.     if(conn->bits.user_passwd) {
```

NULL Pointer Dereference\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4482
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by host at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Line	3523	3468
Object	null	host

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3468.     Curl_safefree(conn->host.rawalloc);
```

NULL Pointer Dereference\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4483
Status	New

The variable declared in null at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3517 is not initialized when it is used by host at curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c in line 3407.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c

Line	3523	3466
Object	null	host

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3523.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_77_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3466.     Curl_free_idnconverted_hostname(&conn->host);
```

NULL Pointer Dereference\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4484
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c in line 753 is not initialized when it is used by cred at curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c in line 753.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	766	845
Object	null	cred

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
766.    struct Curl_schannel_cred *old_cred = NULL;
....
845.                     BACKEND->cred->refcount));
```

NULL Pointer Dereference\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4485

Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c in line 753 is not initialized when it is used by cred at curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c in line 753.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	766	845
Object	null	cred

Code Snippet
File Name   curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method   schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
766.    struct Curl_schannel_cred *old_cred = NULL;
....
845.                     BACKEND->cred->refcount));
```

NULL Pointer Dereference\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4486
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c in line 1797 is not initialized when it is used by state at curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c in line 1797.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c
Line	1801	1842
Object	null	state

Code Snippet
File Name   curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c
Method   CURLcode Curl_retry_request(struct Curl_easy *data, char **url)

```
....
1801.    *url = NULL;
....
1842.            data->state.retrycount);
```

NULL Pointer Dereference\Path 42:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4487
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c in line 1797 is not initialized when it is used by state at curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c in line 1797.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c
Line	1801	1822
Object	null	state

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27774-TP.c
Method	CURLcode Curl_retry_request(struct Curl_easy *data, char **url)

```
....
1801.     *url = NULL;
....
1822.     else if(data->state.refused_stream &&
```

NULL Pointer Dereference\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4488
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c in line 483 is not initialized when it is used by num_connections at curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c in line 88.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c
Line	494	97
Object	null	num_connections

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c
Method	Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
494.     struct connectbundle *bundle_candidate = NULL;
```

File Name	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c
Method	static int bundle_remove_conn(struct connectbundle *bundle,

```
....
97.         bundle->num_connections--;
```

NULL Pointer Dereference\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4489
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c in line 483 is not initialized when it is used by conn_list at curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c in line 88.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c
Line	494	96
Object	null	conn_list

Code Snippet

File Name curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c

Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
494.     struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c

Method static int bundle_remove_conn(struct connectbundle *bundle,

```
....
96.         Curl_llist_remove(&bundle->conn_list, curr, NULL);
```

NULL Pointer Dereference\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4490
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c in line 483 is not initialized when it is used by conn_list at curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c in line 88.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c

Line	494	93
Object	null	conn_list

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c
Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
494.     struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_79_0-CVE-2022-27775-TP.c

Method static int bundle_remove_conn(struct connectbundle *bundle,

```
....
93.     curr = bundle->conn_list.head;
```

NULL Pointer Dereference\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4491
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3546 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3436.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	3552	3503
Object	null	hostname_resolve

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3552.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3503.     Curl_safefree(conn->hostname_resolve);
```

NULL Pointer Dereference\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4492
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3546 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3436.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	3552	3477
Object	null	socks_proxy

Code Snippet

File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3552.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct Curl_easy *data,

```
....
3477.      Curl_safefree(conn->socks_proxy.passwd);
```

NULL Pointer Dereference\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4493
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3546 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3436.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	3552	3475
Object	null	socks_proxy

Code Snippet	
File Name	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3552.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3475.       Curl_safefree(conn->socks_proxy.user);
```

NULL Pointer Dereference\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4494
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3546 is not initialized when it is used by passwd at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3436.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	3552	3463
Object	null	passwd

Code Snippet	
File Name	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method	static CURLcode create_conn(struct Curl_easy *data,

```
....
3552.     struct connectdata *conn_temp = NULL;
```

File Name	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method	static void reuse_conn(struct Curl_easy *data,

```
....
3463.       Curl_safefree(conn->passwd);
```

NULL Pointer Dereference\Path 50:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4495
Status	New

The variable declared in null at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3546 is not initialized when it is used by user at curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c in line 3436.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Line	3552	3462
Object	null	user

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3552.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_79_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct Curl_easy *data,

```
....
3462.       Curl_safefree(conn->user);
```

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=1000014&projectid=9&pathid=4725
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	767	767
Object	pathlen	pathlen

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
767.            co->path[pathlen] = 0; /* null-terminate */
```

Unchecked Array Index\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4726
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1087	1087
Object	myhash	myhash

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	Curl_cookie_add(struct Curl_easy *data,

```
....
1087.        c->cookies[myhash] = co;
```

Unchecked Array Index\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4727
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	216	216
Object	n	n

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	get_alg_id_by_name(char *name)

```
....
216.    tmp[n] = 0;
```

Unchecked Array Index\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4728
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1586	1586
Object	sockindex	sockindex

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c

Method schannel_connect_common(struct Curl_easy *data, struct connectdata *conn,

```
....
1586.       conn->recv[sockindex] = schannel_recv;
```

Unchecked Array Index\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4729
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	1587	1587
Object	sockindex	sockindex

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c

Method schannel_connect_common(struct Curl_easy *data, struct connectdata *conn,

```
....
1587.       conn->send[sockindex] = schannel_send;
```

Unchecked Array Index\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4730

Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	216	216
Object	n	n

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method get_alg_id_by_name(char *name)

```
....
216.     tmp[n] = 0;
```

Unchecked Array Index\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4731
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	1586	1586
Object	sockindex	sockindex

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_common(struct Curl_easy *data, struct connectdata *conn,

```
....
1586.       conn->recv[sockindex] = schannel_recv;
```

Unchecked Array Index\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4732
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c

Line	1587	1587
Object	sockindex	sockindex

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_common(struct Curl_easy *data, struct connectdata *conn,

```
....
1587.       conn->send[sockindex] = schannel_send;
```

Unchecked Array Index\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4733
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	812	812
Object	certnum	certnum

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
812.     ci->certinfo[certnum] = nl;
```

Unchecked Array Index\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4734
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	886	886
Object	stripped_pem_count	stripped_pem_count

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c

Method	static CURLcode pubkey_pem_to_der(const char *pem,

```
....
886.     stripped_pem[stripped_pem_count] = '\0';
```

Unchecked Array Index\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4735
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	213	213
Object	CURL_TELOPT_SGA	CURL_TELOPT_SGA

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	CURLcode init_telnet(struct Curl_easy *data)

```
....
213.     tn->us_preferred[CURL_TELOPT_SGA] = CURL_YES;
```

Unchecked Array Index\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4736
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	214	214
Object	CURL_TELOPT_SGA	CURL_TELOPT_SGA

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	CURLcode init_telnet(struct Curl_easy *data)

```
....
214.     tn->him_preferred[CURL_TELOPT_SGA] = CURL_YES;
```

Unchecked Array Index\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4737
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	221	221
Object	CURL_TELOPT_BINARY	CURL_TELOPT_BINARY

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	CURLcode init_telnet(struct Curl_easy *data)

```
....
221.     tn->us_preferred[CURL_TELOPT_BINARY] = CURL_YES;
```

Unchecked Array Index\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4738
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	222	222
Object	CURL_TELOPT_BINARY	CURL_TELOPT_BINARY

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	CURLcode init_telnet(struct Curl_easy *data)

```
....
222.     tn->him_preferred[CURL_TELOPT_BINARY] = CURL_YES;
```

Unchecked Array Index\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4739
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	243	243
Object	CURL_TELOPT_NAWS	CURL_TELOPT_NAWS

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	CURLcode init_telnet(struct Curl_easy *data)

```
....
243.     tn->subnegotiation[CURL_TELOPT_NAWS] = CURL_YES;
```

Unchecked Array Index\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4740
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	327	327
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void set_remote_option(struct Curl_easy *data, int option, int newstate)

```
....
327.         tn->him[option] = CURL_WANTYES;
```

Unchecked Array Index\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4741
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	339	339

Object	option	option

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void set_remote_option(struct Curl_easy *data, int option, int newstate)

```
....
339.          tn->himq[option] = CURL_OPPOSITE;
```

Unchecked Array Index\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4742
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	353	353
Object	option	option

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void set_remote_option(struct Curl_easy *data, int option, int newstate)

```
....
353.          tn->himq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4743
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	366	366
Object	option	option

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void set_remote_option(struct Curl_easy *data, int option, int newstate)

```
....
366.          tn->him[option] = CURL_WANTNO;
```

Unchecked Array Index\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4744
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	376	376
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void set_remote_option(struct Curl_easy *data, int option, int newstate)

```
....
376.            tn->himq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4745
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	384	384
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void set_remote_option(struct Curl_easy *data, int option, int newstate)

```
....
384.            tn->himq[option] = CURL_OPPOSITE;
```

Unchecked Array Index\Path 22:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4746
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	452	452
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void rec_wont(struct Curl_easy *data, int option)

```
....
452.       tn->him[option] = CURL_NO;
```

Unchecked Array Index\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4747
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	459	459
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void rec_wont(struct Curl_easy *data, int option)

```
....
459.         tn->him[option] = CURL_NO;
```

Unchecked Array Index\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4748
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	463	463
Object	option	option

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void rec_wont(struct Curl_easy *data, int option)

```
....
463.          tn->him[option] = CURL_WANTYES;
```

Unchecked Array Index\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4749
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	464	464
Object	option	option

Code Snippet
File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void rec_wont(struct Curl_easy *data, int option)

```
....
464.          tn->himq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4750
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	473	473

Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void rec_wont(struct Curl_easy *data, int option)

```
....
473.         tn->him[option] = CURL_NO;
```

Unchecked Array Index\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4751
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	476	476
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void rec_wont(struct Curl_easy *data, int option)

```
....
476.         tn->him[option] = CURL_NO;
```

Unchecked Array Index\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4752
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	477	477
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void rec_wont(struct Curl_easy *data, int option)

```
....
477.        tn->himq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4753
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	491	491
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	set_local_option(struct Curl_easy *data, int option, int newstate)

```
....
491.        tn->us[option] = CURL_WANTYES;
```

Unchecked Array Index\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4754
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	503	503
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	set_local_option(struct Curl_easy *data, int option, int newstate)

```
....
503.          tn->usq[option] = CURL_OPPOSITE;
```

Unchecked Array Index\Path 31:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4755
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	517	517
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	set_local_option(struct Curl_easy *data, int option, int newstate)

```
....
517.            tn->usq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4756
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	530	530
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	set_local_option(struct Curl_easy *data, int option, int newstate)

```
....
530.          tn->us[option] = CURL_WANTNO;
```

Unchecked Array Index\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4757
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	540	540
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method set_local_option(struct Curl_easy *data, int option, int newstate)

```
....
540.          tn->usq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4758
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	548	548
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method set_local_option(struct Curl_easy *data, int option, int newstate)

```
....
548.          tn->usq[option] = CURL_OPPOSITE;
```

Unchecked Array Index\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4759
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	628	628

Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void rec_dont(struct Curl_easy *data, int option)

```
....
628.        tn->us[option] = CURL_NO;
```

Unchecked Array Index\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4760
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	635	635
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void rec_dont(struct Curl_easy *data, int option)

```
....
635.          tn->us[option] = CURL_NO;
```

Unchecked Array Index\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4761
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	639	639
Object	option	option

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method void rec_dont(struct Curl_easy *data, int option)

```
....
639.          tn->us[option] = CURL_WANTYES;
```

Unchecked Array Index\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4762
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	640	640
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void rec_dont(struct Curl_easy *data, int option)

```
....
640.          tn->usq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4763
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	649	649
Object	option	option

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	void rec_dont(struct Curl_easy *data, int option)

```
....
649.          tn->us[option] = CURL_NO;
```

Unchecked Array Index\Path 40:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4764
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	652	652
Object	option	option

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c

Method void rec_dont(struct Curl_easy *data, int option)

```
....
652.        tn->us[option] = CURL_NO;
```

Unchecked Array Index\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4765
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	653	653
Object	option	option

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c

Method void rec_dont(struct Curl_easy *data, int option)

```
....
653.        tn->usq[option] = CURL_EMPTY;
```

Unchecked Array Index\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4766
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	795	795
Object	CURL_TELOPT_NEW_ENVIRON	CURL_TELOPT_NEW_ENVIRON

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
795.       tn->us_preferred[CURL_TELOPT_NEW_ENVIRON] = CURL_YES;
```

Unchecked Array Index\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4767
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	806	806
Object	CURL_TELOPT_TTYPE	CURL_TELOPT_TTYPE

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
806.           tn->us_preferred[CURL_TELOPT_TTYPE] = CURL_YES;
```

Unchecked Array Index\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4768
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	814	814

Object	CURL_TELOPT_XDISPLOC	CURL_TELOPT_XDISPLOC

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
814.          tn->us_preferred[CURL_TELOPT_XDISPLOC] = CURL_YES;
```

Unchecked Array Index\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4769
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	826	826
Object	CURL_TELOPT_NEW_ENVIRON	CURL_TELOPT_NEW_ENVIRON

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
826.          tn->us_preferred[CURL_TELOPT_NEW_ENVIRON] = CURL_YES;
```

Unchecked Array Index\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4770
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	834	834
Object	CURL_TELOPT_NAWS	CURL_TELOPT_NAWS

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
834.            tn->us_preferred[CURL_TELOPT_NAWS] = CURL_YES;
```

Unchecked Array Index\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4771
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	847	847
Object	CURL_TELOPT_BINARY	CURL_TELOPT_BINARY

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
847.            tn->us_preferred[CURL_TELOPT_BINARY] = CURL_NO;
```

Unchecked Array Index\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4772
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	848	848
Object	CURL_TELOPT_BINARY	CURL_TELOPT_BINARY

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method	static CURLcode check_telnet_options(struct Curl_easy *data)

```
....
848.            tn->him_preferred[CURL_TELOPT_BINARY] = CURL_NO;
```

Unchecked Array Index\Path 49:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4773
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c	curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Line	1202	1202
Object	j	j

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22925-TP.c
Method static CURLcode send_telnet_data(struct Curl_easy *data,

```
....
1202.       outbuf[j] = '\0';
```

Unchecked Array Index\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4774
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Line	1357	1357
Object	sockindex	sockindex

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27774-TP.c
Method int Curl_single_getsock(struct Curl_easy *data,

```
....
1357.       sock[sockindex] = conn->sockfd;
```

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=1000014&projectid=9&

	pathid=4640
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1142	1142
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1142.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4641
Status	New

The cookie_output method in curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1545	1545
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	static int cookie_output(struct Curl_easy *data,

```
....
1545.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 3:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4642
Status	New

The schannel_connect_step1 method in curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	633	633
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
633.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

TOCTOU\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4643
Status	New

The schannel_connect_step1 method in curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Line	633	633
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method	schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
633.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

TOCTOU\Path 5:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4644
Status	New

The Curl_pin_peer_pubkey method in curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	985	985
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
985.     fp = fopen(pinnedpubkey, "rb");
```

TOCTOU\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4645
Status	New

The vms_realfilesize method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	169	169
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static curl_off_t vms_realfilesize(const char *name,

```
....
169.     file = fopen(name, "r"); /* VMS */
```

TOCTOU\Path 7:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4646
Status	New

The single_transfer method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	899	899
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
899.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

TOCTOU\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4647
Status	New

The single_transfer method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	936	936
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
936.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

TOCTOU\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4648
Status	New

The single_transfer method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	978	978
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
978.              FILE *newfile = fopen(config->etag_save_file, "wb");
```

TOCTOU\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4649
Status	New

The single_transfer method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1116	1116
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1116.              FILE *file = fopen(outfile, "ab",
```

TOCTOU\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4650
Status	New

The single_transfer method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1600	1600
Object	fopen	fopen

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1600.              FILE *fInCert = fopen(config->cert + 8, "rb");
```

TOCTOU\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4651
Status	New

The single_transfer method in curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1643	1643
Object	fopen	fopen

Code Snippet	
File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c

Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1643.              FILE *fInCert = fopen(config->key + 8, "rb");
```

TOCTOU\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4652
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1188	1188
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1188.      fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4653
Status	New

The cookie_output method in curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1605	1605
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1605.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4654
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1188	1188
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1188.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4655
Status	New

The cookie_output method in curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1605	1605
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1605.        out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4656
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1188	1188
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method	struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1188.        fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4657
Status	New

The cookie_output method in curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1605	1605
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1605.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4658
Status	New

The schannel_acquire_credential_handle method in curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	542	542
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
542.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

TOCTOU\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4659
Status	New

The schannel_acquire_credential_handle method in curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	542	542

Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
542.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

TOCTOU\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4660
Status	New

The Curl_pin_peer_pubkey method in curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	1014	1014
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1014.    fp = fopen(pinnedpubkey, "rb");
```

TOCTOU\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4661
Status	New

The vms_realfilesize method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c

Line	168	168
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
168.     file = fopen(name, "r"); /* VMS */
```

TOCTOU\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4662
Status	New

The single_transfer method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	832	832
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
832.             newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

TOCTOU\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4663
Status	New

The single_transfer method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	869	869
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
869.                FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

TOCTOU\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4664
Status	New

The single_transfer method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	911	911
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
911.                  FILE *newfile = fopen(config->etag_save_file, "wb");
```

TOCTOU\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4665
Status	New

The single_transfer method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	1034	1034
Object	fopen	fopen

Code Snippet
File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1034.                   FILE *file = fopen(outfile, "ab",
```

TOCTOU\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4666
Status	New

The single_transfer method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	1511	1511
Object	fopen	fopen

Code Snippet
File Name	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1511.                   FILE *fInCert = fopen(config->cert + 8, "rb");
```

TOCTOU\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4667
Status	New

The single_transfer method in curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	1554	1554
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1554.              FILE *fInCert = fopen(config->key + 8, "rb");
```

TOCTOU\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4668
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1196	1196
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.      fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4669
Status	New

The cookie_output method in curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1614	1614
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4670
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1196	1196
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4671
Status	New

The cookie_output method in curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1614	1614
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4672
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1196	1196
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4673
Status	New

The cookie_output method in curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1614	1614
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4674
Status	New

The schannel_acquire_credential_handle method in curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	541	541
Object	fopen	fopen

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
541.           fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

TOCTOU\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4675
Status	New

The schannel_acquire_credential_handle method in curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	541	541
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
541.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

TOCTOU\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4676
Status	New

The Curl_pin_peer_pubkey method in curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	1022	1022
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1022.     fp = fopen(pinnedpubkey, "rb");
```

TOCTOU\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4677
Status	New

The vms_realfilesize method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	168	168
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
168.     file = fopen(name, "r"); /* VMS */
```

TOCTOU\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4678
Status	New

The single_transfer method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	850	850
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
850.             FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

TOCTOU\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4679
Status	New

The single_transfer method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	890	890
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
890.            FILE *newfile = fopen(config->etag_save_file, "wb");
```

TOCTOU\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4680
Status	New

The single_transfer method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	945	945
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
945.            newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

TOCTOU\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4681

Status	New

The single_transfer method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	1077	1077
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1077.              FILE *file = fopen(outfile, "ab",
```

TOCTOU\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4682
Status	New

The single_transfer method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	1572	1572
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1572.              FILE *fInCert = fopen(config->cert + 8, "rb");
```

TOCTOU\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=4683
Status	New

The single_transfer method in curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	1615	1615
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1615.                FILE *fInCert = fopen(config->key + 8, "rb");
```

TOCTOU\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4684
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1196	1196
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.      fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 46:

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

	[PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4685]()
Status	New

The cookie_output method in curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1614	1614
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 47:

Severity	Low
Result State	To Verify
Online Results	[http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4686]()
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1196	1196
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 48:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4687
Status	New

The cookie_output method in curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1614	1614
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

TOCTOU\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4688
Status	New

The *Curl_cookie_init method in curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1196	1196
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

TOCTOU\Path 50:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4689
Status	New

The cookie_output method in curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c file utilizes fopen 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	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1614	1614
Object	fopen	fopen

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

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=1000014&projectid=9&pathid=4364
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1346	1346
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1346.       array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4365
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1356	1356
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1356.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4366
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1560	1560
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method	static int cookie_output(struct Curl_easy *data,

```
....
1560.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4367
Status	New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1574	1574
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1574.       qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4368
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	766	766
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
766.     table = calloc((size_t) num, sizeof(struct curl_slist *));
```

Use of Sizeof On a Pointer Type\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4369
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1414	1414

Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1414.       array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4370
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1424	1424
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1424.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4371
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1622	1622
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1622.        array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4372
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1637	1637
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1637.        qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4373
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1414	1414
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1414.        array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4374
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1424	1424
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1424.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4375
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1622	1622
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1622.      array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4376
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1637	1637
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1637.       qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4377
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1414	1414
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1414.       array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4378
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1424	1424

Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1424.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4379
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1622	1622
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1622.      array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4380
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1637	1637
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1637.       qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4381
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	795	795
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
795.    table = calloc((size_t) num, sizeof(struct curl_slist *));
```

Use of Sizeof On a Pointer Type\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4382
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1423	1423
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1423.       array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4383
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1433	1433
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1433.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4384
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1631	1631
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1631.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4385
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1646	1646
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4386
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1423	1423
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1423.      array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4387
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1433	1433

Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1433.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4388
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1631	1631
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1631.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4389
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1646	1646
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4390
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1423	1423
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1423.      array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4391
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1433	1433
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1433.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4392
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1631	1631
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1631.        array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4393
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1646	1646
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.        qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4394
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	803	803
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
803.    table = calloc((size_t) num, sizeof(struct curl_slist *));
```

Use of Sizeof On a Pointer Type\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4395
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1423	1423
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1423.      array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4396
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1433	1433

Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1433.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4397
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1631	1631
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1631.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4398
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1646	1646
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4399
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1423	1423
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1423.      array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4400
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1433	1433
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1433.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4401
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1631	1631
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1631.      array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4402
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1646	1646
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4403
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1423	1423
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1423.       array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4404
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1433	1433
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1433.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4405
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1631	1631

Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1631.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4406
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1646	1646
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1646.       qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4407
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Line	1426	1426
Object	sizeof	sizeof

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Method	struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1426.       array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4408
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Line	1436	1436
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1436.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4409
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Line	1634	1634
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1634.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Use of Sizeof On a Pointer Type\Path 47:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4410
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Line	1649	1649
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1649.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

Use of Sizeof On a Pointer Type\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4411
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Line	1426	1426
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1426.      array = malloc(sizeof(struct Cookie *) * matches);
```

Use of Sizeof On a Pointer Type\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4412
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Line	1436	1436
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1436.        qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

Use of Sizeof On a Pointer Type\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4413
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Line	1634	1634
Object	sizeof	sizeof

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1634.        array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

Incorrect Permission Assignment For Critical Resources

Query Path:
CPP\Cx\CPP Low Visibility\Incorrect Permission Assignment For Critical Resources Version:1

Categories

FISMA 2014: Access Control
NIST SP 800-53: AC-3 Access Enforcement (P1)
OWASP Top 10 2017: A2-Broken Authentication

Description

Incorrect Permission Assignment For Critical Resources\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

pathid=4075
Status New

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Line	1545	1545
Object	out	out

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1545.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 2:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4076
Status New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Line	633	633
Object	fInCert	fInCert

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22890-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
633.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 3:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4077
Status New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c

Line	633	633
Object	fInCert	fInCert

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22901-FP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
633.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4078
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	985	985
Object	fp	fp

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
985.     fp = fopen(pinnedpubkey, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4079
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	169	169
Object	file	file

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c

Method static curl_off_t vms_realfilesize(const char *name,

```
....
169.     file = fopen(name, "r"); /* VMS */
```

Incorrect Permission Assignment For Critical Resources\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4080
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	899	899
Object	newfile	newfile

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
899.            newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

Incorrect Permission Assignment For Critical Resources\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4081
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Line	1605	1605
Object	out	out

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1605.      out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4082
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c
Line	1605	1605
Object	out	out

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-32205-TP.c

Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1605.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4083
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c
Line	1605	1605
Object	out	out

Code Snippet

File Name curl@@curl-curl-7_77_0-CVE-2022-35252-TP.c

Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1605.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4084
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Line	542	542
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
542.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4085
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Line	542	542
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2021-22901-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
542.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4086
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	1014	1014

Object	fp	fp

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1014.     fp = fopen(pinnedpubkey, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4087
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	168	168
Object	file	file

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
168.     file = fopen(name, "r"); /* VMS */
```

Incorrect Permission Assignment For Critical Resources\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4088
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	832	832
Object	newfile	newfile

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
832.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

Incorrect Permission Assignment For Critical Resources\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4089
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Line	1614	1614
Object	out	out

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27779-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4090
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Line	1614	1614
Object	out	out

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-32205-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4091
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c
Line	1614	1614
Object	out	out

Code Snippet

File Name curl@@curl-curl-7_79_0-CVE-2022-35252-TP.c

Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4092
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c
Line	541	541
Object	fInCert	fInCert

Code Snippet

File Name curl@@curl-curl-7_81_0-CVE-2021-22890-FP.c

Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
541.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4093
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Line	541	541
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2021-22901-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
541.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4094
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	1022	1022
Object	fp	fp

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1022.     fp = fopen(pinnedpubkey, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4095
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	168	168

Object	file	file

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
168.     file = fopen(name, "r"); /* VMS */
```

Incorrect Permission Assignment For Critical Resources\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4096
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Line	945	945
Object	newfile	newfile

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
945.                 newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

Incorrect Permission Assignment For Critical Resources\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4097
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Line	1614	1614
Object	out	out

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-27779-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4098
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Line	1614	1614
Object	out	out

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-32205-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4099
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Line	1614	1614
Object	out	out

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-35252-TP.c
Method	static CURLcode cookie_output(struct Curl_easy *data,

```
....
1614.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 26:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4100
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c
Line	546	546
Object	fInCert	fInCert

Code Snippet

File Name curl@@curl-curl-7_83_0-CVE-2021-22890-FP.c

Method schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
546.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4101
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Line	166	166
Object	file	file

Code Snippet

File Name curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c

Method static curl_off_t vms_realfilesize(const char *name,

```
....
166.    file = fopen(name, "r"); /* VMS */
```

Incorrect Permission Assignment For Critical Resources\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4102
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Line	941	941
Object	newfile	newfile

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
941.                  newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

Incorrect Permission Assignment For Critical Resources\Path 29:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4103
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Line	1196	1196
Object	fp	fp

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = fopen(file, FOPEN_READTEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 30:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4104
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c	curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Line	1617	1617

Object	out	out

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-27779-FP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1617.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4105
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Line	1196	1196
Object	fp	fp

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = fopen(file, FOPEN_READTEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4106
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c	curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Line	1617	1617
Object	out	out

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-32205-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1617.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4107
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_83_0-CVE-2022-35252-TP.c
Line	1196	1196
Object	fp	fp

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-35252-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1196.       fp = fopen(file, FOPEN_READTEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4108
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-35252-TP.c	curl@@curl-curl-7_83_0-CVE-2022-35252-TP.c
Line	1617	1617
Object	out	out

Code Snippet
File Name curl@@curl-curl-7_83_0-CVE-2022-35252-TP.c
Method static CURLcode cookie_output(struct Curl_easy *data,

```
....
1617.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 35:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4109
Status	New

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Line	602	602
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_easy *data,

```
....
602.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 36:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4110
Status	New

	Source	Destination
File	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Line	81	81
Object	file	file

Code Snippet

File Name	curl@@curl-curl-7_85_0-CVE-2022-35260-TP.c
Method	static int parsenetrc(const char *host,

```
....
81.     file = fopen(netrcfile, FOPEN_READTEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4111
Status	New

	Source	Destination
File	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c	curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Line	603	603
Object	fInCert	fInCert

Code Snippet
File Name curl@@curl-curl-7_87_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
603.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4112
Status	New

	Source	Destination
File	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Line	608	608
Object	fInCert	fInCert

Code Snippet
File Name curl@@curl-curl-8_1_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
608.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4113
Status	New

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Line	608	608

Object	fInCert	fInCert

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
608.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4114
Status	New

	Source	Destination
File	curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c	curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c
Line	82	82
Object	file	file

Code Snippet
File Name curl@@curl-curl-8_3_0-CVE-2023-52071-TP.c
Method bool tool_create_output_file(struct OutStruct *outs,

```
....
82.       file = fopen(fname, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 41:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4115
Status	New

	Source	Destination
File	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Line	573	573
Object	fInCert	fInCert

Code Snippet
File Name curl@@curl-curl-8_6_0-CVE-2021-22890-FP.c
Method schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
573.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 42:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4116
Status	New

	Source	Destination
File	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Line	573	573
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-8_8_0-CVE-2021-22890-FP.c
Method	schannel_acquire_credential_handle(struct Curl_cfilter *cf,

```
....
573.          fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 43:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4117
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	936	936
Object	file	file

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
936.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 44:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4118
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	978	978
Object	newfile	newfile

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
978.            FILE *newfile = fopen(config->etag_save_file, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 45:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4119
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1116	1116
Object	file	file

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1116.            FILE *file = fopen(outfile, "ab",
```

Incorrect Permission Assignment For Critical Resources\Path 46:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4120
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1600	1600
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1600.            FILE *fInCert = fopen(config->cert + 8, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 47:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4121
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Line	1643	1643
Object	fInCert	fInCert

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-27778-TP.c
Method	static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1643.            FILE *fInCert = fopen(config->key + 8, "rb");
```

Incorrect Permission Assignment For Critical Resources\Path 48:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4122
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	869	869

Object	file	file

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
869.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

Incorrect Permission Assignment For Critical Resources\Path 49:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4123
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	911	911
Object	newfile	newfile

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
911.              FILE *newfile = fopen(config->etag_save_file, "wb");
```

Incorrect Permission Assignment For Critical Resources\Path 50:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4124
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Line	1034	1034
Object	file	file

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1034.                   FILE *file = fopen(outfile, "ab",
```

Potential Off by One Error in Loops

Query Path:
CPP\Cx\CPP Heuristic\Potential Off by One Error in Loops Version:1

Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

Description

Potential Off by One Error in Loops\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3117
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 318 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	367	367
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
367.        for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3118
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 318 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	371	371
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
371.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3119
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 318 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	396	396
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
396.            for (j = 0; j <= wc; 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=1000014&projectid=9&pathid=3120
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 318 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	419	419
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
419.            for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3121
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	1670	1670
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1670.        for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3122
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	1674	1674
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1674.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3123
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	1699	1699
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1699.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3124
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c at line 1621 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	1722	1722
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1722.           for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3125
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	370	370
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
370.        for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3126
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	374	374
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
374.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3127
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	399	399
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
399.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3128
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	422	422
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
422.            for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3129
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	1678	1678
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1678.       for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3130
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	1682	1682
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1682.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3131
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	1707	1707
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1707.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 16:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3132
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	1730	1730
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1730.           for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3133
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	370	370
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
370.       for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3134
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	374	374
Object	<=	<=

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	blockconvLow(l_uint32 *data,

```
....
374.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3135
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	399	399
Object	<=	<=

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	blockconvLow(l_uint32 *data,

```
....
399.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3136
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 321 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	422	422
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
422.             for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3137
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	1678	1678
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1678.       for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3138
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	1682	1682
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1682.           for (j = 0; j <= wc; 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=1000014&projectid=9&pathid=3139
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	1707	1707
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1707.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3140
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c at line 1629 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	1730	1730
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1730.          for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3141
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	364	364
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
364.      for (i = 0; i <= hc; i++) {    /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3142
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	368	368
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
368.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3143
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	393	393
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
393.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3144
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	416	416
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
416.            for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 29:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3145
Status New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	1645	1645
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1645.        for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 30:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3146
Status New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	1649	1649
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1649.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 31:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3147
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	1674	1674
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1674.           for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 32:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3148
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	1697	1697
Object	<=	<=

Code Snippet

File Name	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method	blocksumLow(l_uint32 *datad,

```
....
1697.           for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 33:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3149
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	364	364
Object	<=	<=

Code Snippet

File Name	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method	blockconvLow(l_uint32 *data,

```
....
364.        for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 34:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3150
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	368	368
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
368.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 35:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3151
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	393	393
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
393.            for (j = 0; j <= wc; 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=1000014&projectid=9&pathid=3152
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 317 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	416	416
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blockconvLow(l_uint32 *data,

```
....
416.            for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Potential Off by One Error in Loops\Path 37:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3153
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	1645	1645
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1645.       for (i = 0; i <= hc; i++) {     /* first hc + 1 lines */
```

Potential Off by One Error in Loops\Path 38:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3154
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	1649	1649
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1649.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 39:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3155
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	1674	1674
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1674.            for (j = 0; j <= wc; j++) {
```

Potential Off by One Error in Loops\Path 40:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3156
Status	New

The buffer allocated by <= in DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c at line 1598 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

	Source	Destination

File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	1697	1697
Object	<=	<=

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method blocksumLow(l_uint32 *datad,

```
....
1697.            for (j = 0; j <= wc; j++) {    /* first wc + 1 columns */
```

Sizeof Pointer Argument

Query Path:
CPP\Cx\CPP Low Visibility\Sizeof Pointer Argument Version:0

Description

Sizeof Pointer Argument\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3184
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	330	330
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3185
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c

Line	330	330
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3186
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	366	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3187
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	330	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3188
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	347	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3189
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	366	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3190
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	330	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3191
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	347	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.        for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
366.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3192
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	330	330
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.      for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3193
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	330	330
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.      for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3194
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	366	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3195
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	330	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=3196
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	347	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.        for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
366.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3197
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	366	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
366.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3198
Status	New

	Source	Destination

File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	330	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 16:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3199
Status New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	347	366
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
366.     for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 17:

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3200
Status New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c

Line	1318	1318
Object	backends	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method static size_t multissl_version(char *buffer, size_t size)

```
....
1318.       char *end = backends + sizeof(backends);
```

Sizeof Pointer Argument\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3201
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	347	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3202
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	330	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3203
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	347	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3204
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	330	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3205
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	1347	1347
Object	backends	sizeof

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method	static size_t multissl_version(char *buffer, size_t size)

```
....
1347.      char *end = backends + sizeof(backends);
```

Sizeof Pointer Argument\Path 23:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3206
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	347	347
Object	cipherlist	sizeof

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method	static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3207
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	330	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3208
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	347	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=3209
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	330	347
Object	cipherlist	sizeof

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
330.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
347.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

Sizeof Pointer Argument\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3210
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	1355	1355
Object	backends	sizeof

Code Snippet
File Name curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method static size_t multissl_version(char *buffer, size_t size)

```
....
1355.       char *end = backends + sizeof(backends);
```

Sizeof Pointer Argument\Path 28:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3211
Status	New

	Source	Destination

File	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c	dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Line	114	114
Object	ip_buf	sizeof

Code Snippet
File Name dlundquist@@sniproxy-0.6.1-CVE-2023-25076-TP.c
Method new_address(const char *hostname_or_ip) {

```
....
114.          if (len < sizeof(ip_buf) && port_num >= 0 && port_num <=
65535) {
```

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=1000014&projectid=9&pathid=3157
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 128 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 128 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c
Line	132	132
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c
Method buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
132.      sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3158
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 138 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 138 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c
Line	142	142
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c
Method parseError(DcmTagKey t)

```
....
142.        sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3159
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 148 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 148 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c
Line	152	152
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2021-41689-TP.c

Method parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
152.      sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3160
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 128 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 128 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c
Line	132	132
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c
Method buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
132.      sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3161
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 138 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 138 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c

Line	142	142
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c
Method parseError(DcmTagKey t)

```
....
142.       sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3162
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 148 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 148 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c
Line	152	152
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34508-TP.c
Method parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
152.       sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3163
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 128 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 128 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c
Line	132	132
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c
Method	buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
132.        sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3164
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 138 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 138 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c
Line	142	142
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c
Method	parseError(DcmTagKey t)

```
....
142.        sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 9:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3165
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 148 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 148 of DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c
Line	152	152
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.6-CVE-2024-34509-FP.c
Method	parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
152.       sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3166
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c
Line	125	125
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c
Method	buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
125.        sprintf(buf, "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s",
```

Potential Precision Problem\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3167
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c
Line	135	135
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c
Method parseError(DcmTagKey t)

```
....
135.        sprintf(buf, "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s",
```

Potential Precision Problem\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3168
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c
Line	145	145

Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2021-41689-FP.c
Method parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
145.       sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3169
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c
Line	125	125
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c
Method buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
125.       sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 14:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3170
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to

"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c
Line	135	135
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c
Method parseError(DcmTagKey t)

```
....
135.        sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 15:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3171
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c
Line	145	145
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34508-TP.c
Method parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
145.        sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 16:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3172
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c
Line	125	125
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c
Method	buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
125.        sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 17:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3173
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c
Line	135	135
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c
Method	parseError(DcmTagKey t)

```
....
135.       sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 18:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3174
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c
Line	145	145
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.7-CVE-2024-34509-FP.c
Method	parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
145.       sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 19:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3175
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c
Line	125	125

Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c
Method buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
125.       sprintf(buf, "DIMSE: Command Build Failed: %s: Element: 
(%04x,%04x) %s",
```

Potential Precision Problem\Path 20:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3176
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c
Line	135	135
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet
File Name DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c
Method parseError(DcmTagKey t)

```
....
135.       sprintf(buf, "DIMSE: Command Parse Failed: Element: 
(%04x,%04x) %s",
```

Potential Precision Problem\Path 21:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3177
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c
Line	145	145
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2021-41689-FP.c
Method	parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
145.        sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 22:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3178
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c
Line	125	125
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c
Method	buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
125.        sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 23:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3179
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c
Line	135	135
Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c
Method	parseError(DcmTagKey t)

```
....
135.       sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 24:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3180
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c
Line	145	145
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34508-TP.c
Method	parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
145.       sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Potential Precision Problem\Path 25:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3181
Status	New

The size of the buffer used by buildErrorWithMsg in "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that buildErrorWithMsg passes to "DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s", at line 121 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c
Line	125	125
Object	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Build Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c
Method	buildErrorWithMsg(const char* msg, DcmTagKey t)

```
....
125.       sprintf(buf, "DIMSE: Command Build Failed: %s: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 26:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3182
Status	New

The size of the buffer used by parseError in "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseError passes to "DIMSE: Command Parse Failed: Element: (%04x,%04x) %s", at line 131 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c
Line	135	135

Object	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c
Method	parseError(DcmTagKey t)

```
....
135.       sprintf(buf, "DIMSE: Command Parse Failed: Element:
(%04x,%04x) %s",
```

Potential Precision Problem\Path 27:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=3183
Status	New

The size of the buffer used by parseErrorWithMsg in "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that parseErrorWithMsg passes to "DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s", at line 141 of DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c, to overwrite the target buffer.

	Source	Destination
File	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c
Line	145	145
Object	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"	"DIMSE: Command Parse Failed: %s: Element: (%04x,%04x) %s"

Code Snippet

File Name	DCMTK@@dcmtk-DCMTK-3.6.8-CVE-2024-34509-TP.c
Method	parseErrorWithMsg(const char* msg, DcmTagKey t)

```
....
145.       sprintf(buf, "DIMSE: Command Parse Failed: %s: Element:
(%04x,%04x) %s", msg,
```

Use of Insufficiently Random Values

Query Path:
CPP\Cx\CPP Low Visibility\Use of Insufficiently Random Values Version:0

Categories

FISMA 2014: Media Protection
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)
OWASP Top 10 2017: A3-Sensitive Data Exposure

Description

Use of Insufficiently Random Values\Path 1:

Severity	Low

Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4146
Status	New

Method gaussDistribSampling at line 2549 of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	2557	2557
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2557.                 frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4147
Status	New

Method gaussDistribSampling at line 2549 of DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Line	2559	2559
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.80.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2559.                 frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 3:

Severity	Low
Result State	To Verify

Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4148
Status	New

Method gaussDistribSampling at line 2557 of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	2565	2565
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2565.                   frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4149
Status	New

Method gaussDistribSampling at line 2557 of DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Line	2567	2567
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.81.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2567.                   frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 5:

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

	PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4150
Status	New

Method gaussDistribSampling at line 2557 of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	2565	2565
Object	rand	rand

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	gaussDistribSampling(void)

```
....
2565.               frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 6:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4151
Status	New

Method gaussDistribSampling at line 2557 of DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Line	2567	2567
Object	rand	rand

Code Snippet

File Name	DanBloomberg@@leptonica-1.82.0-CVE-2022-38266-FP.c
Method	gaussDistribSampling(void)

```
....
2567.               frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 7:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&

	pathid=4152
Status	New

Method gaussDistribSampling at line 2506 of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	2514	2514
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2514.               frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 8:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4153
Status	New

Method gaussDistribSampling at line 2506 of DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Line	2516	2516
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.83.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2516.               frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 9:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4154

Status	New

Method gaussDistribSampling at line 2506 of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	2514	2514
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2514.            frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 10:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4155
Status	New

Method gaussDistribSampling at line 2506 of DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c uses a weak method rand to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c	DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Line	2516	2516
Object	rand	rand

Code Snippet
File Name DanBloomberg@@leptonica-1.84.0-CVE-2022-38266-FP.c
Method gaussDistribSampling(void)

```
....
2516.            frand = (l_float32)rand() / (l_float32)RAND_MAX;
```

Use of Insufficiently Random Values\Path 11:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4156
Status	New

Method Curl_ssl_random at line 830 of curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c uses a weak method random to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Line	834	834
Object	random	random

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2021-22924-FP.c
Method	CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
834.    return Curl_ssl->random(data, entropy, length);
```

Use of Insufficiently Random Values\Path 12:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4157
Status	New

Method Curl_ssl_random at line 859 of curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c uses a weak method random to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Line	863	863
Object	random	random

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
863.    return Curl_ssl->random(data, entropy, length);
```

Use of Insufficiently Random Values\Path 13:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4158
Status	New

Method Curl_ssl_random at line 867 of curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c uses a weak method random to produce random values. These values might be used for secret values, personal identifiers or cryptographic input, allowing an attacker to guess the value.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Line	871	871
Object	random	random

Code Snippet
File Name	curl@@curl-curl-7_81_0-CVE-2022-22576-TP.c
Method	CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
871.     return Curl_ssl->random(data, entropy, length);
```

Exposure of System Data to Unauthorized Control Sphere

Query Path:
CPP\Cx\CPP Low Visibility\Exposure of System Data to Unauthorized Control Sphere Version:1

Categories

FISMA 2014: Configuration Management
NIST SP 800-53: AC-3 Access Enforcement (P1)

Description

Exposure of System Data to Unauthorized Control Sphere\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4137
Status	New

The system data read by krb5_auth in the file curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c at line 206 is potentially exposed by krb5_auth found in curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c at line 206.

	Source	Destination
File	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Line	230	230
Object	perror	perror

Code Snippet
File Name	curl@@curl-curl-7_75_0-CVE-2022-32208-TP.c
Method	krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
230.       perror("getsockname()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4138
Status	New

The system data read by krb5_auth in the file curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c at line 196 is potentially exposed by krb5_auth found in curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c at line 196.

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c
Line	220	220
Object	perror	perror

Code Snippet

File Name	curl@@curl-curl-7_77_0-CVE-2022-32208-TP.c
Method	krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
220.        perror("getsockname()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4139
Status	New

The system data read by krb5_auth in the file curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c at line 196 is potentially exposed by krb5_auth found in curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c at line 196.

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c
Line	220	220
Object	perror	perror

Code Snippet

File Name	curl@@curl-curl-7_79_0-CVE-2022-32208-TP.c
Method	krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
220.        perror("getsockname()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4140
Status	New

The system data read by krb5_auth in the file curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c at line 196 is potentially exposed by krb5_auth found in curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c at line 196.

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c
Line	220	220
Object	perror	perror

Code Snippet

File Name curl@@curl-curl-7_81_0-CVE-2022-32208-TP.c

Method krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
220.      perror("getsockname()");
```

Exposure of System Data to Unauthorized Control Sphere\Path 5:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4141
Status	New

The system data read by krb5_auth in the file curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c at line 190 is potentially exposed by krb5_auth found in curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c at line 190.

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c	curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c
Line	214	214
Object	perror	perror

Code Snippet

File Name curl@@curl-curl-7_83_0-CVE-2022-32208-TP.c

Method krb5_auth(void *app_data, struct Curl_easy *data, struct connectdata *conn)

```
....
214.      perror("getsockname()");
```

Information Exposure Through Comments

Query Path:

CPP\Cx\CPP Low Visibility\Information Exposure Through Comments Version:1

Categories

FISMA 2014: Identification And Authentication
NIST SP 800-53: SC-28 Protection of Information at Rest (P1)

Description

Information Exposure Through Comments\Path 1:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4142
Status	New

	Source	Destination
File	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Line	380	380
Object	cipher-	cipher-

Code Snippet
File Name curl@@curl-curl-7_77_0-CVE-2022-27781-TP.c
Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....
380.    * Return true if at least one cipher-suite is enabled. Used to
determine
```

Information Exposure Through Comments\Path 2:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4143
Status	New

	Source	Destination
File	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Line	380	380
Object	cipher-	cipher-

Code Snippet
File Name curl@@curl-curl-7_79_0-CVE-2022-27781-TP.c
Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....
380.    * Return true if at least one cipher-suite is enabled. Used to
determine
```

Information Exposure Through Comments\Path 3:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4144
Status	New

	Source	Destination
File	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Line	382	382
Object	cipher-	cipher-

Code Snippet

File Name	curl@@curl-curl-7_81_0-CVE-2022-27781-TP.c
Method	* Return true if at least one cipher-suite is enabled. Used to determine

```
....
382.    * Return true if at least one cipher-suite is enabled. Used to
determine
```

Information Exposure Through Comments\Path 4:

Severity	Low
Result State	To Verify
Online Results	http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000014&projectid=9&pathid=4145
Status	New

	Source	Destination
File	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Line	382	382
Object	cipher-	cipher-

Code Snippet

File Name	curl@@curl-curl-7_83_0-CVE-2022-27781-TP.c
Method	* Return true if at least one cipher-suite is enabled. Used to determine

```
....
382.    * Return true if at least one cipher-suite is enabled. Used to
determine
```

Buffer Overflow LongString

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

CPP

Overflowing Buffers

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

Checked Buffers

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

Format String Attack

Risk

What might happen

In environments with unmanaged memory, allowing attackers to control format strings could enable them to access areas of memory to which they should not have access, including reading other restricted variables, misrepresenting data, and possibly even overwriting unauthorized areas of memory. It is even possible this could further lead to buffer overflows and arbitrary code execution under certain circumstance.

Cause

How does it happen

The application allows user input to influence the string argument used for formatted print functions. This family of functions expects the first argument to designate the relative format of dynamically constructed output string, including how to represent each of the other arguments.

Allowing an external user or attacker to control this string, allows them to control the functioning of the printing function, and thus to access unexpected areas of memory.

General Recommendations

How to avoid it

Generic Guidance:

- Do not allow user input or any other external data to influence the format strings.
- Ensure that all string format functions are called with a static string as the format parameter, and that the correct number of arguments are passed to the function, according to the static format string.
- Alternatively, validate all user input before using it in the format string parameter to print format functions, and ensure formatting tokens are not included in the input.

Specific Recommendations:

- Do not include user input directly in the format string parameter (often the first or second argument) to formatting functions.
- Alternatively, use controlled information derived from the input, such as size or length, in the format string - but not the actual contents of the input itself.

Source Code Examples

CPP

Dynamic Formatting String - First Parameter of printf

```
printf("Hello, ");
printf(name); // If name contains tokens, it could retrieve arbitrary values from memory or
```

```
cause a crash
```

Static Formatting String - First Parameter of printf is Static

```
printf("Hello, %s", name);
```

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 OutOfBound

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

Divide By Zero

Risk

What might happen

When a program divides a number by zero, an exception will be raised. If this exception is not handled by the application, unexpected results may occur, including crashing the application. This can be considered a DoS (Denial of Service) attack, if an external user has control of the value of the denominator or can cause this error to occur.

Cause

How does it happen

The program receives an unexpected value, and uses it for division without filtering, validation, or verifying that the value is not zero. The application does not explicitly handle this error or prevent division by zero from occuring.

General Recommendations

How to avoid it

- Before dividing by an unknown value, validate the number and explicitly ensure it does not evaluate to zero.
- Validate all untrusted input from all sources, in particular verifying that it is not zero before dividing with it.
- Verify output of methods, calculations, dictionary lookups, and so on, and ensure it is not zero before dividing with the result.
- Ensure divide-by-zero errors are caught and handled appropriately.

Source Code Examples

Java

Divide by Zero

```
public float getAverage(HttpServletRequest req) {
     int total = Integer.parseInt(req.getParameter("total"));
     int count = Integer.parseInt(req.getParameter("count"));

     return total / count;
}
```

Checked Division

```
public float getAverage(HttpServletRequest req) {
     int total = Integer.parseInt(req.getParameter("total"));
     int count = Integer.parseInt(req.getParameter("count"));
```

```
      if (count > 0)
            return total / count;
      else
            return 0;
}
```

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);
```

Boolean 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

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

```c
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

Heap Inspection

Risk

What might happen

All variables stored by the application in unencrypted memory can potentially be retrieved by an unauthorized user, with privlieged access to the machine. For example, a privileged attacker could attach a debugger to the running process, or retrieve the process's memory from the swapfile or crash dump file.
Once the attacker finds the user passwords in memory, these can be reused to easily impersonate the user to the system.

Cause

How does it happen

String variables are immutable - in other words, once a string variable is assigned, its value cannot be changed or removed. Thus, these strings may remain around in memory, possibly in multiple locations, for an indefinite period of time until the garbage collector happens to remove it. Sensitive data, such as passwords, will remain exposed in memory as plaintext with no control over their lifetime.

General Recommendations

How to avoid it

Generic Guidance:

- Do not store senstiive data, such as passwords or encryption keys, in memory in plaintext, even for a short period of time.
- Prefer to use specialized classes that store encrypted memory.
- Alternatively, store secrets temporarily in mutable data types, such as byte arrays, and then promptly zeroize the memory locations.

Specific Recommendations - Java:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SealedObject.

Specific Recommendations - .NET:

- Instead of storing passwords in immutable strings, prefer to use an encrypted memory object, such as SecureString or ProtectedData.

Source Code Examples

Java

Plaintext Password in Immutable String

```
class Heap_Inspection
{
  private string password;

  void setPassword()
```

```
 {
      password = System.console().readLine("Enter your password: ");
  }
}
```

Password Protected in Memory

```
class Heap_Inspection_Fixed
{
  private SealedObject password;

  void setPassword()
 {
      byte[] sKey = getKeyFromConfig();
      Cipher c = Cipher.getInstance("AES");
      c.init(Cipher.ENCRYPT_MODE, sKey);

      char[] input = System.console().readPassword("Enter your password: ");
      password = new SealedObject(Arrays.asList(input), c);

    //Zero out the possible password, for security.
    Arrays.fill(password, '0');
  }
}
```

CPP

Vulnerable C code

```
/* Vulnerable to heap inspection */

#include <stdio.h>


void somefunc(){
      printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
        char* password = (char *) malloc(256);
        char ch;
        ssize_t k;
            int i=0;
        while(k = read(0, &ch, 1) > 0)
        {
                if (ch == '\n'){
                        password[i]='\0';
                        break;
                } else{
                        password[i++]=ch;
                        fflush(0);
                }
        }
        printf("Password: %s\n",&password[0]);
}

int main()

{

    printf("Please enter a password:\n");

      authfunc();
      printf("You can now dump memory to find this password!");
      somefunc();
      gets();

}
```

Safe C code

```
/* Pesumably safe heap */

#include <stdio.h>
#include <string.h>

#define STDIN_FILENO 0

void somefunc(){
        printf("Yea, I'm just being called for the heap of it..\n");
}

void authfunc(){
      char* password = (char*) malloc(256);
      int i=0;
      char ch;
      ssize_t k;
      while(k = read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n'){
                    password[i]='\0';
                    break;
             } else{
                    password[i++]=ch;
                    fflush(0);
             }
      }
      i=0;
      memset(password,'\0',256);
}

int main()

{

      printf("Please enter a password:\n");
      authfunc();
      somefunc();
      char ch;
      while(read(STDIN_FILENO, &ch, 1) > 0)
      {
             if (ch == '\n')
                    break;
      }
}
```

Inadequate Encryption Strength

Risk

What might happen

Using weak or outdated cryptography does not provide sufficient protection for sensitive data. An attacker that gains access to the encrypted data would likely be able to break the encryption, using either cryptanalysis or brute force attacks. Thus, the attacker would be able to steal user passwords and other personal data. This could lead to user impersonation or identity theft.

Cause

How does it happen

The application uses a weak algorithm, that is considered obselete since it is relatively easy to break. These obselete algorithms are vulnerable to several different kinds of attacks, including brute force.

General Recommendations

How to avoid it

Generic Guidance:

- Always use strong, modern algorithms for encryption, hashing, and so on.
- Do not use weak, outdated, or obsolete algorithms.
- Ensure you select the correct cryptographic mechanism according to the specific requirements.
- Passwords should be protected with a dedicated password protection scheme, such as bcrypt, scrypt, PBKDF2, or Argon2.

Specific Recommendations:

- Do not use SHA-1, MD5, or any other weak hash algorithm to protect passwords or personal data. Instead, use a stronger hash such as SHA-256 when a secure hash is required.
- Do not use DES, Triple-DES, RC2, or any other weak encryption algorithm to protect passwords or personal data. Instead, use a stronger encryption algorithm such as AES to protect personal data.
- Do not use weak encryption modes such as ECB, or rely on insecure defaults. Explicitly specify a stronger encryption mode, such as GCM.
- For symmetric encryption, use a key length of at least 256 bits.

Source Code Examples

Java

Weakly Hashed PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.md5Hex(socialSecurityNum);
}
```

Stronger Hash for PII

```
string protectSSN(HttpServletRequest req) {
    string socialSecurityNum = req.getParameter("SocialSecurityNo");

    return DigestUtils.sha256Hex(socialSecurityNum);
}
```

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**

```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

Wrong Memory 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

Potential Off by One Error in Loops

Risk

What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

Cause

How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

General Recommendations

How to avoid it

- Always ensure that a given iteration boundary is correct:
    - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
    - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

Source Code Examples

CPP

Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
     ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
}
```

Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

Potential Precision Problem

Risk

What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

Cause

How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.

Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

General Recommendations

How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

Source Code Examples

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

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

Incorrect Permission Assignment for Critical Resource

Weakness ID: 732 *(Weakness Class)* **Status:** Draft

Description

Description Summary

The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Extended Description

When a resource is given a permissions setting that provides access to a wider range of actors than required, it could lead to the disclosure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution or sensitive user data.

Time of Introduction

- Architecture and Design
- Implementation
- Installation
- Operation

Applicable Platforms

Languages

Language-independent

Modes of Introduction

The developer may set loose permissions in order to minimize problems when the user first runs the program, then create documentation stating that permissions should be tightened. Since system administrators and users do not always read the documentation, this can result in insecure permissions being left unchanged.

The developer might make certain assumptions about the environment in which the software runs - e.g., that the software is running on a single-user system, or the software is only accessible to trusted administrators. When the software is running in a different environment, the permissions become a problem.

Common Consequences

Scope	Effect
Confidentiality	An attacker may be able to read sensitive information from the associated resource, such as credentials or configuration information stored in a file.
Integrity	An attacker may be able to modify critical properties of the associated resource to gain privileges, such as replacing a world-writable executable with a Trojan horse.
Availability	An attacker may be able to destroy or corrupt critical data in the associated resource, such as deletion of records from a database.

Likelihood of Exploit

Medium to High

Detection Methods

Automated Static Analysis

Automated static analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc. Automated techniques may be able to detect the use of library functions that modify permissions, then analyze function calls for arguments that contain potentially insecure values.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated static analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated static analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Automated Dynamic Analysis

Automated dynamic analysis may be effective in detecting permission problems for system resources such as files, directories, shared memory, device interfaces, etc.

However, since the software's intended security policy might allow loose permissions for certain operations (such as publishing a file on a web server), automated dynamic analysis may produce some false positives - i.e., warnings that do not have any security consequences or require any code changes.

When custom permissions models are used - such as defining who can read messages in a particular forum in a bulletin board system - these can be difficult to detect using automated dynamic analysis. It may be possible to define custom signatures that identify any custom functions that implement the permission checks and assignments.

Manual Static Analysis

Manual static analysis may be effective in detecting the use of custom permissions models and functions. The code could then be examined to identifying usage of the related functions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Manual Dynamic Analysis

Manual dynamic analysis may be effective in detecting the use of custom permissions models and functions. The program could then be executed with a focus on exercising code paths that are related to the custom permissions. Then the human analyst could evaluate permission assignments in the context of the intended security model of the software.

Fuzzing

Fuzzing is not effective in detecting this weakness.

Demonstrative Examples

Example 1

The following code sets the umask of the process to 0 before creating a file and writing "Hello world" into the file.

(Bad Code)

Example Language: **C**

```
#define OUTFILE "hello.out"

umask(0);
FILE *out;
/* Ignore CWE-59 (link following) for brevity */
out = fopen(OUTFILE, "w");
if (out) {
fprintf(out, "hello world!\n");
fclose(out);
}
```

After running this program on a UNIX system, running the "ls -l" command might return the following output:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 hello.out
```

The "rw-rw-rw-" string indicates that the owner, group, and world (all users) can read the file and write to it.

Example 2

The following code snippet might be used as a monitor to periodically record whether a web site is alive. To ensure that the file can always be modified, the code uses chmod() to make the file world-writable.

(Bad Code)

Example Language: **Perl**

```
$fileName = "secretFile.out";

if (-e $fileName) {
chmod 0777, $fileName;
}
```

```
my $outFH;
if (! open($outFH, ">>$fileName")) {
ExitError("Couldn't append to $fileName: $!");
}
my $dateString = FormatCurrentTime();
my $status = IsHostAlive("cwe.mitre.org");
print $outFH "$dateString cwe status: $status!\n";
close($outFH);
```

The first time the program runs, it might create a new file that inherits the permissions from its environment. A file listing might look like:

(Result)

```
-rw-r--r-- 1 username 13 Nov 24 17:58 secretFile.out
```

This listing might occur when the user has a default umask of 022, which is a common setting. Depending on the nature of the file, the user might not have intended to make it readable by everyone on the system.

The next time the program runs, however - and all subsequent executions - the chmod will set the file's permissions so that the owner, group, and world (all users) can read the file and write to it:

(Result)

```
-rw-rw-rw- 1 username 13 Nov 24 17:58 secretFile.out
```

Perhaps the programmer tried to do this because a different process uses different permissions that might prevent the file from being updated.

Example 3

The following command recursively sets world-readable permissions for a directory and all of its children:

(Bad Code)

Example Language: **Shell**

```
chmod -R ugo+r DIRNAME
```

If this command is run from a program, the person calling the program might not expect that all the files under the directory will be world-readable. If the directory is expected to contain private data, this could become a security problem.

Observed Examples

Reference	Description
CVE-2009-3482	Anti-virus product sets insecure "Everyone: Full Control" permissions for files under the "Program Files" folder, allowing attackers to replace executables with Trojan horses.
CVE-2009-3897	Product creates directories with 0777 permissions at installation, allowing users to gain privileges and access a socket used for authentication.
CVE-2009-3489	Photo editor installs a service with an insecure security descriptor, allowing users to stop or start the service, or execute commands as SYSTEM.
CVE-2009-3289	Library function copies a file to a new target and uses the source file's permissions for the target, which is incorrect when the source file is a symbolic link, which typically has 0777 permissions.
CVE-2009-0115	Device driver uses world-writable permissions for a socket file, allowing attackers to inject arbitrary commands.
CVE-2009-1073	LDAP server stores a cleartext password in a world-readable file.
CVE-2009-0141	Terminal emulator creates TTY devices with world-writable permissions, allowing an attacker to write to the terminals of other users.

CVE-2008-0662	VPN product stores user credentials in a registry key with "Everyone: Full Control" permissions, allowing attackers to steal the credentials.
CVE-2008-0322	Driver installs its device interface with "Everyone: Write" permissions.
CVE-2009-3939	Driver installs a file with world-writable permissions.
CVE-2009-3611	Product changes permissions to 0777 before deleting a backup; the permissions stay insecure for subsequent backups.
CVE-2007-6033	Product creates a share with "Everyone: Full Control" permissions, allowing arbitrary program execution.
CVE-2007-5544	Product uses "Everyone: Full Control" permissions for memory-mapped files (shared memory) in inter-process communication, allowing attackers to tamper with a session.
CVE-2005-4868	Database product uses read/write permissions for everyone for its shared memory, allowing theft of credentials.
CVE-2004-1714	Security product uses "Everyone: Full Control" permissions for its configuration files.
CVE-2001-0006	"Everyone: Full Control" permissions assigned to a mutex allows users to disable network connectivity.
CVE-2002-0969	Chain: database product contains buffer overflow that is only reachable through a .ini configuration file - which has "Everyone: Full Control" permissions.

Potential Mitigations

Phase: Implementation

When using a critical resource such as a configuration file, check to see if the resource has insecure permissions (such as being modifiable by any regular user), and generate an error or even exit the software if there is a possibility that the resource could have been modified by an unauthorized party.

Phase: Architecture and Design

Divide your application into anonymous, normal, privileged, and administrative areas. Reduce the attack surface by carefully defining distinct user groups, privileges, and/or roles. Map these against data, functionality, and the related resources. Then set the permissions accordingly. This will allow you to maintain more fine-grained control over your resources.

Phases: Implementation; Installation

During program startup, explicitly set the default permissions or umask to the most restrictive setting possible. Also set the appropriate permissions during program installation. This will prevent you from inheriting insecure permissions from any user who installs or runs the program.

Phase: System Configuration

For all configuration files, executables, and libraries, make sure that they are only readable and writable by the software's administrator.

Phase: Documentation

Do not suggest insecure configuration changes in your documentation, especially if those configurations can extend to resources and other software that are outside the scope of your own software.

Phase: Installation

Do not assume that the system administrator will manually change the configuration to the settings that you recommend in the manual.

Phase: Testing

Use 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. These may be more effective than strictly automated techniques. This is especially the case with weaknesses that are related to design and business rules.

Phase: Testing

Use monitoring tools that examine the software's process as it interacts with the operating system and the network. This technique is useful in cases when source code is unavailable, if the software was not developed by you, or if you want to verify that the build phase did not introduce any new weaknesses. Examples include debuggers that directly attach to the running process; system-call tracing utilities such as truss (Solaris) and strace (Linux); system activity monitors such as FileMon, RegMon, Process Monitor, and other Sysinternals utilities (Windows); and sniffers and protocol analyzers that monitor network traffic.

Attach the monitor to the process and watch for library functions or system calls on OS resources such as files, directories, and shared memory. Examine the arguments to these calls to infer which permissions are being used.

Note that this technique is only useful for permissions issues related to system resources. It is not likely to detect application-level business rules that are related to permissions, such as if a user of a blog system marks a post as "private," but the blog system inadvertently marks it as "public."

Phases: Testing; System Configuration

Ensure that your software runs properly under the Federal Desktop Core Configuration (FDCC) or an equivalent hardening configuration guide, which many organizations use to limit the attack surface and potential risk of deployed software.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	275	Permission Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	668	Exposure of Resource to Wrong Sphere	**Research Concepts (primary)1000**
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**
RequiredBy	Compound Element: Composite	689	Permission Race Condition During Resource Copy	Research Concepts1000
ParentOf	Weakness Variant	276	Incorrect Default Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	277	Insecure Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	278	Insecure Preserved Inherited Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Variant	279	Incorrect Execution-Assigned Permissions	**Research Concepts (primary)1000**
ParentOf	Weakness Base	281	Improper Preservation of Permissions	**Research Concepts (primary)1000**

Related Attack Patterns

CAPEC-ID	Attack Pattern Name	*(CAPEC Version: 1.5)*
232	Exploitation of Privilege/Trust	
1	Accessing Functionality Not Properly Constrained by ACLs	
17	Accessing, Modifying or Executing Executable Files	
60	Reusing Session IDs (aka Session Replay)	
61	Session Fixation	
62	Cross Site Request Forgery (aka Session Riding)	
122	Exploitation of Authorization	
180	Exploiting Incorrectly Configured Access Control Security Levels	
234	Hijacking a privileged process	

References

Mark Dowd, John McDonald and Justin Schuh. "The Art of Software Security Assessment". Chapter 9, "File Permissions." Page 495.. 1st Edition. Addison Wesley. 2006.

John Viega and Gary McGraw. "Building Secure Software". Chapter 8, "Access Control." Page 194.. 1st Edition. Addison-Wesley. 2002.

Maintenance Notes

The relationships between privileges, permissions, and actors (e.g. users and groups) need further refinement within the Research view. One complication is that these concepts apply to two different pillars, related to control of resources (CWE-664) and protection mechanism failures (CWE-396).

Content History

Submissions

Submission Date	Submitter	Organization	Source
2008-09-08			Internal CWE Team
	new weakness-focused entry for Research view.		

Modifications

Modification Date	Modifier	Organization	Source
2009-01-12	CWE Content Team	MITRE	Internal
	updated Description, Likelihood of Exploit, Name, Potential Mitigations, Relationships		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		
2009-05-27	CWE Content Team	MITRE	Internal
	updated Name		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Demonstrative Examples, Detection Factors, Modes of Introduction, Observed Examples, Potential Mitigations, References		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		
2010-04-05	CWE Content Team	MITRE	Internal
	updated Potential Mitigations, Related Attack Patterns		

Previous Entry Names

Change Date	Previous Entry Name
2009-01-12	Insecure Permission Assignment for Resource
2009-05-27	Insecure Permission Assignment for Critical Resource

BACK TO TOP

Exposure of System Data to Unauthorized Control Sphere

Risk

What might happen

System data can provide attackers with valuable insights on systems and services they are targeting - any type of system data, from service version to operating system fingerprints, can assist attackers to hone their attack, correlate data with known vulnerabilities or focus efforts on developing new attacks against specific technologies.

Cause

How does it happen

System data is read and subsequently exposed where it might be read by untrusted entities.

General Recommendations

How to avoid it

Consider the implications of exposure of the specified input, and expected level of access to the specified output. If not required, consider removing this code, or modifying exposed information to exclude potentially sensitive system data.

Source Code Examples

Java

Leaking Environment Variables in JSP Web-Page

```
String envVarValue = System.getenv(envVar);
if (envVarValue == null) {
    out.println("Environment variable is not defined:");
    out.println(System.getenv());
} else {
    //[..]
};
```

Information Leak Through Comments

Weakness ID: 615 *(Weakness Variant)* **Status:** Incomplete

Description

Description Summary

While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

Extended Description

An attacker who finds these comments can map the application's structure and files, expose hidden parts of the site, and study the fragments of code to reverse engineer the application, which may help develop further attacks against the site.

Time of Introduction

- Implementation

Demonstrative Examples

Example 1

The following comment, embedded in a JSP, will be displayed in the resulting HTML output.

(Bad Code)

Example Languages: **HTML and JSP**

```
<!-- FIXME: calling this with more than 30 args kills the JDBC server -->
```

Observed Examples

Reference	Description
CVE-2007-6197	Version numbers and internal hostnames leaked in HTML comments.
CVE-2007-4072	CMS places full pathname of server in HTML comment.
CVE-2009-2431	blog software leaks real username in HTML comment.

Potential Mitigations

Remove comments which have sensitive information about the design/implementation of the application. Some of the comments may be exposed to the user and affect the security posture of the application.

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Weakness Variant	540	Information Leak Through Source Code	**Development Concepts (primary)699** **Research Concepts (primary)1000**

Content History

Submissions			
Submission Date	**Submitter**	**Organization**	**Source**
	Anonymous Tool Vendor (under NDA)		Externally Mined

Modifications			
Modification Date	**Modifier**	**Organization**	**Source**
2008-07-01	Sean Eidemiller	Cigital	External
	added/updated demonstrative examples		
2008-07-01	Eric Dalci	Cigital	External
	updated Potential Mitigations, Time of Introduction		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2008-10-14	CWE Content Team	MITRE	Internal
	updated Description		
2009-03-10	CWE Content Team	MITRE	Internal

	updated Demonstrative Examples		
2009-07-27	CWE Content Team	MITRE	Internal
	updated Observed Examples, Taxonomy Mappings		

BACK TO TOP

Use of Insufficiently Random Values

Risk

What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

Cause

How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.

Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

General Recommendations

How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

Source Code Examples

Java

Use of a weak pseudo-random number generator

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

Cryptographically secure random number generator

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

Objc

Use of a weak pseudo-random number generator

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

Cryptographically secure random number generator

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

Swift

Use of a weak pseudo-random number generator

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

Cryptographically secure random number generator

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

Unchecked Return Value

Risk

What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

Cause

How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

General Recommendations

How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

Source Code Examples

CPP

Unchecked Memory Allocation

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

Safer Memory Allocation

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

Use of sizeof() on a Pointer Type

Weakness ID: 467 *(Weakness Variant)* **Status:** Draft

Description

Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

Time of Introduction

- Implementation

Applicable Platforms

Languages

C

C++

Common Consequences

Scope	Effect
Integrity	This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows.

Likelihood of Exploit

High

Demonstrative Examples

Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

(Bad Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

(Good Code)

Example Languages: **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

(Bad Code)

```

/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

(Attack)

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

Potential Mitigations

Phase: Implementation

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

Weakness Ordinalities

Ordinality	Description
Primary	*(where the weakness exists independent of other weaknesses)*

Relationships

Nature	Type	ID	Name	View(s) this relationship pertains to
ChildOf	Category	465	Pointer Issues	**Development Concepts (primary)699**
ChildOf	Weakness Class	682	Incorrect Calculation	**Research Concepts (primary)1000**
ChildOf	Category	737	CERT C Secure Coding Section 03 - Expressions (EXP)	**Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734**
ChildOf	Category	740	CERT C Secure Coding Section 06 - Arrays (ARR)	Weaknesses Addressed by the CERT C Secure Coding Standard734
CanPrecede	Weakness Base	131	Incorrect Calculation of Buffer Size	Research Concepts1000

Taxonomy Mappings

Mapped Taxonomy Name	Node ID	Fit	Mapped Node Name
CLASP			Use of sizeof() on a pointer type
CERT C Secure Coding	ARR01-C		Do not apply the sizeof operator to a pointer when taking the size of an array
CERT C Secure Coding	EXP01-C		Do not take the size of a pointer to determine the size of the pointed-to type

White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

Content History

Submissions

Submission Date	Submitter	Organization	Source
	CLASP		Externally Mined

Modifications

Modification Date	Modifier	Organization	Source
2008-07-01	Eric Dalci	Cigital	External
	updated Time of Introduction		
2008-08-01		KDM Analytics	External
	added/updated white box definitions		
2008-09-08	CWE Content Team	MITRE	Internal
	updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities		
2008-11-24	CWE Content Team	MITRE	Internal
	updated Relationships, Taxonomy Mappings		
2009-03-10	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2009-12-28	CWE Content Team	MITRE	Internal
	updated Demonstrative Examples		
2010-02-16	CWE Content Team	MITRE	Internal
	updated Relationships		

BACK TO TOP

NULL Pointer Dereference

Risk

What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

Cause

How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

General Recommendations

How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

Source Code Examples

CPP

Explicit NULL Dereference

```
char * input = NULL;
printf("%s", input);
```

Implicit NULL Dereference

```
char * input;
printf("%s", input);
```

Java

Explicit Null Dereference

```
Object o = null;
out.println(o.getClass());
```

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