# vul_files_6 Scan Report

| | |
|---|---|
| Project Name | vul_files_6 |
| Scan Start | Monday, January 6, 2025 4:07:37 PM |
| Preset | Checkmarx Default |
| Scan Time | 02h:08m:56s |
| Lines Of Code Scanned | 299212 |
| Files Scanned | 142 |
| Report Creation Time | Monday, January 6, 2025 6:39:09 PM |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8 |
| Team | CxServer |
| Checkmarx Version | 8.7.0 |
| Scan Type | Full |
| Source Origin | LocalPath |
| Density | 1/100 (Vulnerabilities/LOC) |
| Visibility | Public |

# Filter Settings

**Severity**

Included: High, Medium, Low, Information

Excluded: None

**Result State**

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

Excluded: None

**Assigned to**

Included: All

**Categories**

Included:

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

Excluded:

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

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

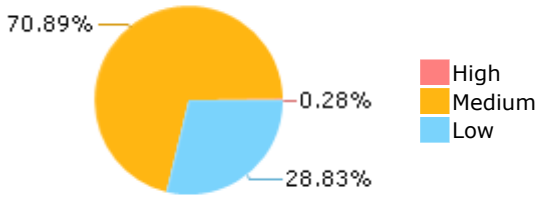
**Results Limit**

Results limit per query was set to 50

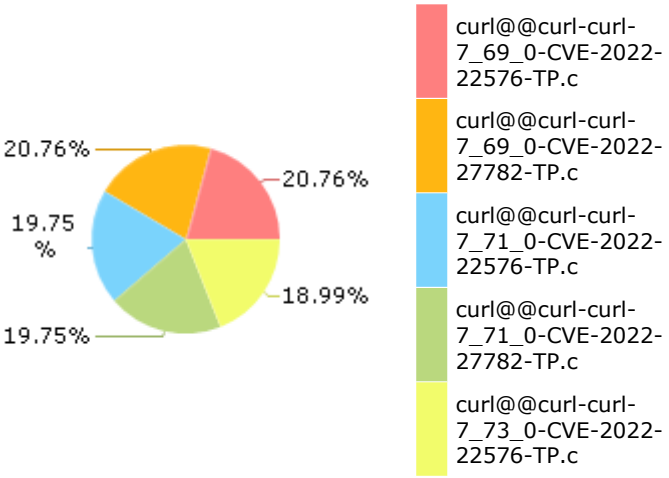
**Selected Queries**

Selected queries are listed in Result Summary

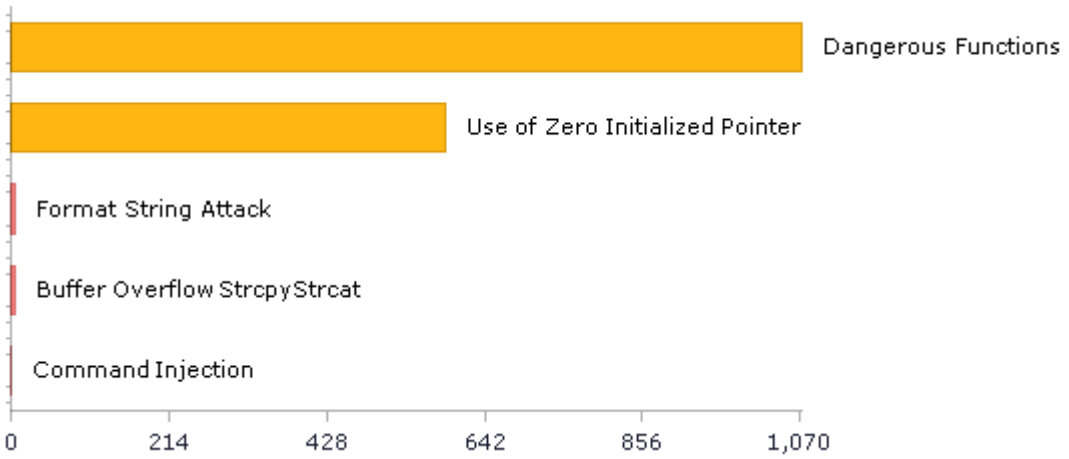
## Result Summary




## Most Vulnerable Files




## Top 5 Vulnerabilities



# Scan Summary - OWASP Top 10 2017

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

| Category | Threat Agent | Exploitability | Weakness Prevalence | Weakness Detectability | Technical Impact | Business Impact | Issues Found | Best Fix Locations |
|---|---|---|---|---|---|---|---|---|
| A1-Injection | App. Specific | EASY | COMMON | EASY | SEVERE | App. Specific | 532 | 380 |
| A2-Broken Authentication | App. Specific | EASY | COMMON | AVERAGE | SEVERE | App. Specific | 345 | 345 |
| A3-Sensitive Data Exposure | App. Specific | AVERAGE | WIDESPREAD | AVERAGE | SEVERE | App. Specific | 31 | 24 |
| 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 | 1072 | 1072 |
| 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 | 1 | 1 |
| 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 | 13 | 13 |
| 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 | 1072 | 1072 |
| 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 | 11 | 11 |
| PCI DSS (3.2) - 6.5.2 - Buffer overflows | 357 | 357 |
| 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. | 69 | 69 |
| 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. | 35 | 28 |
| 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. | 284 | 284 |
| 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. | 17 | 17 |
| 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. | 32 | 32 |

***** 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) | 366 | 366 |
| 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) | 14 | 7 |
| 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) | 12 | 12 |
| SC-4 Information in Shared Resources (P1) | 13 | 13 |
| SC-5 Denial of Service Protection (P1)* | 1206 | 738 |
| SC-8 Transmission Confidentiality and Integrity (P1) | 0 | 0 |
| SI-10 Information Input Validation (P1)* | 273 | 273 |
| SI-11 Error Handling (P2)* | 207 | 207 |
| SI-15 Information Output Filtering (P0) | 0 | 0 |
| SI-16 Memory Protection (P1) | 48 | 36 |

***** 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:<br>-Failing to identify the user at all when that should be required<br>-Failure to maintain the user's identity when it is required<br>-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.).<br>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 |

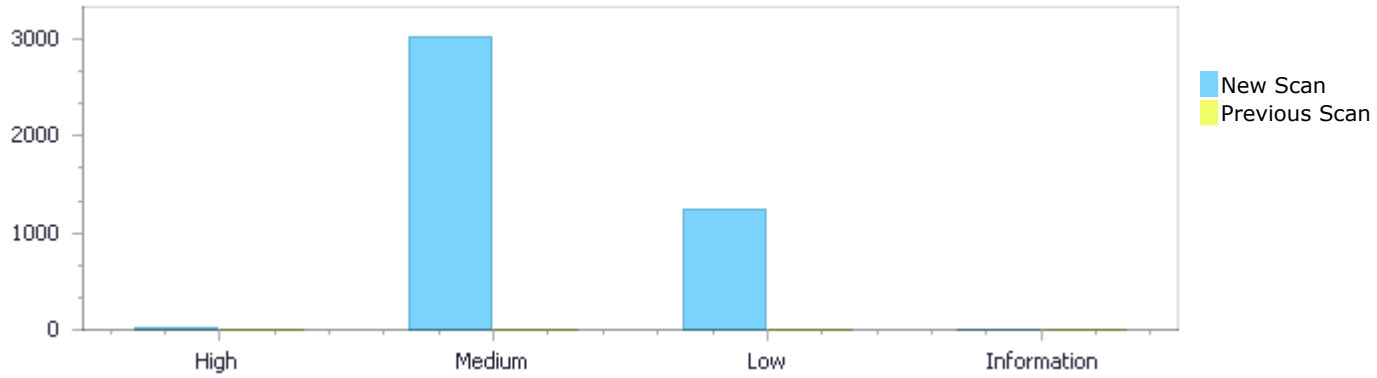
| | | | |
|---|---|---|---|
| | modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain. | | |
| M9-Reverse Engineering | This category includes analysis of the final core binary to determine 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 | 12 | 3,029 | 1,232 | 0 | 4,273 |
| Recurrent Issues | 0 | 0 | 0 | 0 | 0 |
| Total | 12 | 3,029 | 1,232 | 0 | 4,273 |
| | | | | | |
| 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 | 12 | 3,029 | 1,232 | 0 | 4,273 |
| Urgent | 0 | 0 | 0 | 0 | 0 |
| Proposed Not Exploitable | 0 | 0 | 0 | 0 | 0 |
| Total | 12 | 3,029 | 1,232 | 0 | 4,273 |

## Result Summary

| Vulnerability Type | Occurrences | Severity |
|---|---|---|
| Format String Attack | 6 | High |
| Buffer Overflow StrcpyStrcat | 5 | High |
| Command Injection | 1 | High |
| Dangerous Functions | 1072 | Medium |
| Use of Zero Initialized Pointer | 588 | Medium |

| | | |
|---|---|---|
| Memory Leak | 410 | Medium |
| MemoryFree on StackVariable | 387 | Medium |
| Buffer Overflow boundcpy WrongSizeParam | 298 | Medium |
| Wrong Size t Allocation | 165 | Medium |
| Double Free | 34 | Medium |
| Integer Overflow | 23 | Medium |
| Inadequate Encryption Strength | 14 | Medium |
| Heap Inspection | 13 | Medium |
| Boolean Overflow | 8 | Medium |
| Buffer Overflow AddressOfLocalVarReturned | 7 | Medium |
| Char Overflow | 6 | Medium |
| Off by One Error in Methods | 4 | Medium |
| Improper Resource Access Authorization | 276 | Low |
| Unchecked Array Index | 224 | Low |
| Unchecked Return Value | 207 | Low |
| NULL Pointer Dereference | 201 | Low |
| TOCTOU | 91 | Low |
| Incorrect Permission Assignment For Critical Resources | 69 | Low |
| Use of Sizeof On a Pointer Type | 65 | Low |
| Sizeof Pointer Argument | 52 | Low |
| Exposure of System Data to Unauthorized Control Sphere | 21 | Low |
| Potential Off by One Error in Loops | 10 | Low |
| Information Exposure Through Comments | 8 | Low |
| Inconsistent Implementations | 4 | Low |
| Use of Insufficiently Random Values | 4 | Low |

# 10 Most Vulnerable Files

## High and Medium Vulnerabilities

| File Name | Issues Found |
|---|---|
| curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | 64 |
| curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c | 64 |
| curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c | 61 |
| curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c | 60 |
| curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c | 56 |
| curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c | 56 |
| curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | 55 |
| curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | 55 |
| curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c | 53 |
| curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c | 53 |

# Scan Results Details

## 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=1000013&projectid=8&pathid=1 |
| Status | New |

Method check_telnet_options at line 818 of curl@@curl-curl-7_71_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_71_0-CVE-2021-22925-TP.c at line 818.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22925-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22925-TP.c |
| Line | 844 | 844 |
| Object | "%127[^= ]%*[ =]%255s" | "%127[^= ]%*[ =]%255s" |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct connectdata *conn)

```
....
844.      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=1000013&projectid=8&pathid=2 |
| Status | New |

Method check_telnet_options at line 818 of curl@@curl-curl-7_71_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_71_0-CVE-2021-22925-TP.c at line 818.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22925-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22925-TP.c |
| Line | 877 | 877 |
| Object | "%hu%*[xX]%hu" | "%hu%*[xX]%hu" |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct connectdata *conn)

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

**Format String Attack\Path 3:**

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3
Status New

Method check_telnet_options at line 773 of curl@@curl-curl-7_73_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_73_0-CVE-2021-22925-TP.c at line 773.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22925-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22925-TP.c |
| Line | 799 | 799 |
| Object | "%127[^= ]%*[ =]%255s" | "%127[^= ]%*[ =]%255s" |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct connectdata *conn)

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

**Format String Attack\Path 4:**

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4
Status New

Method check_telnet_options at line 773 of curl@@curl-curl-7_73_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_73_0-CVE-2021-22925-TP.c at line 773.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22925-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22925-TP.c |
| Line | 832 | 832 |
| Object | "%hu%*[xX]%hu" | "%hu%*[xX]%hu" |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct connectdata *conn)

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

**Format String Attack\Path 5:**

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=5
Status New

Method check_telnet_options at line 772 of curl@@curl-curl-7_75_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_75_0-CVE-2021-22925-TP.c at line 772.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22925-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22925-TP.c |
| Line | 798 | 798 |
| Object | "%127[^= ]%*[ =]%255s" | "%127[^= ]%*[ =]%255s" |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

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

**Format String Attack\Path 6:**

Severity High
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=6
Status New

Method check_telnet_options at line 772 of curl@@curl-curl-7_75_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_75_0-CVE-2021-22925-TP.c at line 772.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22925-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22925-TP.c |
| Line | 831 | 831 |
| Object | "%hu%*[xX]%hu" | "%hu%*[xX]%hu" |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22925-TP.c
Method static CURLcode check_telnet_options(struct Curl_easy *data)

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

## 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=1000013&projectid=8&pathid=7 |
| Status | New |

The size of the buffer used by Curl_multissl_version in buffer, at line 1230 of curl@@curl-curl-7_69_0-CVE-2021-22924-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_multissl_version passes to buffer, at line 1230 of curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 1230 | 1270 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method static size_t Curl_multissl_version(char *buffer, size_t size)

```
....
1230.  static size_t Curl_multissl_version(char *buffer, size_t size)
....
1270.    strcpy(buffer, backends);
```

**Buffer Overflow StrcpyStrcat\Path 2:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=8 |
| Status | New |

The size of the buffer used by Curl_multissl_version in buffer, at line 1259 of curl@@curl-curl-7_71_0-CVE-2021-22924-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_multissl_version passes to buffer, at line 1259 of curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 1259 | 1299 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method static size_t Curl_multissl_version(char *buffer, size_t size)

```
....
1259.  static size_t Curl_multissl_version(char *buffer, size_t size)
....
1299.    strcpy(buffer, backends);
```

**Buffer Overflow StrcpyStrcat\Path 3:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=9 |
| Status | New |

The size of the buffer used by Curl_multissl_version in buffer, at line 1305 of curl@@curl-curl-7_73_0-CVE-2021-22924-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_multissl_version passes to buffer, at line 1305 of curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 1305 | 1345 |
| Object | buffer | buffer |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Method | static size_t Curl_multissl_version(char *buffer, size_t size) |

```
....
1305.  static size_t Curl_multissl_version(char *buffer, size_t size)
....
1345.    strcpy(buffer, backends);
```

**Buffer Overflow StrcpyStrcat\Path 4:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=10 |
| Status | New |

The size of the buffer used by Curl_sec_read_msg in buffer, at line 685 of curl@@curl-curl-7_73_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 685 of curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c |
| Line | 685 | 735 |
| Object | buffer | buffer |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c |
| Method | int Curl_sec_read_msg(struct connectdata *conn, char *buffer, |

```
....
685.  int Curl_sec_read_msg(struct connectdata *conn, char *buffer,
....
735.    strcpy(buffer, buf);
```

**Buffer Overflow StrcpyStrcat\Path 5:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=11 |
| Status | New |

The size of the buffer used by multissl_version in buffer, at line 1276 of curl@@curl-curl-7_75_0-CVE-2021-22924-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 1276 of curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021- | curl@@curl-curl-7_75_0-CVE-2021- |

| | | |
|---|---|---|
| | 22924-TP.c | 22924-TP.c |
| Line | 1276 | 1316 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method static size_t multissl_version(char *buffer, size_t size)

```
....
1276.  static size_t multissl_version(char *buffer, size_t size)
....
1316.    strcpy(buffer, backends);
```

## Command Injection

Query Path:
CPP\Cx\CPP High Risk\Command Injection Version:1

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection
OWASP Top 10 2013: A1-Injection
FISMA 2014: System And Information Integrity
NIST SP 800-53: SI-10 Information Input Validation (P1)
OWASP Top 10 2017: A1-Injection

*Description*
**Command Injection\Path 1:**

| | |
|---|---|
| Severity | High |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=12 |
| Status | New |

The application's main method calls an OS (shell) command with system, at line 191 of COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c, using an untrusted string with the command to execute.
This could allow an attacker to inject an arbitrary command, and enable a Command Injection attack.

The attacker may be able to inject the executed command via user input, argv, which is retrieved by the application in the main method, at line 191 of COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 191 | 374 |
| Object | argv | system |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
191.  int main(int argc, char *argv[])
....
374.              syserr = system(command);
```

## 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=1000013&projectid=8&pathid=524 |
| Status | New |

The dangerous function, _tcslen, was found in use at line 359 in curl@@curl-curl-7_69_0-CVE-2021-22897-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_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 407 | 407 |
| Object | _tcslen | _tcslen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
407.    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=1000013&projectid=8&pathid=525 |
| Status | New |

The dangerous function, _tcslen, was found in use at line 350 in curl@@curl-curl-7_71_0-CVE-2021-22897-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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 398 | 398 |
| Object | _tcslen | _tcslen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
398.    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=1000013&projectid=8&pathid=526
Status New

The dangerous function, _tcslen, was found in use at line 352 in curl@@curl-curl-7_73_0-CVE-2021-22897-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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 394 | 394 |
| Object | _tcslen | _tcslen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
394.    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=1000013&projectid=8&pathid=527
Status New

The dangerous function, _tcslen, was found in use at line 353 in curl@@curl-curl-7_75_0-CVE-2021-22897-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-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 395 | 395 |
| Object | _tcslen | _tcslen |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method get_cert_location(TCHAR *path, DWORD *store_name, TCHAR **store_path,

```
....
395.    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=1000013&projectid=8&pathid=528
Status New

The dangerous function, memcpy, was found in use at line 131 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 157 | 157 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_volumeheader(cli_ctx *ctx, hfsPlusVolumeHeader **header)

```
....
157.      memcpy(volHeader, mPtr, 512);
```

**Dangerous Functions\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=529
Status New

The dangerous function, memcpy, was found in use at line 212 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 254 | 254 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.      memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

**Dangerous Functions\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=530 |
| Status | New |

The dangerous function, memcpy, was found in use at line 212 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 267 | 267 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.      memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

**Dangerous Functions\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=531 |
| Status | New |

The dangerous function, memcpy, was found in use at line 479 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 529 | 529 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], unsigned *recordSize)

```
....
529.          memcpy(&nodeDesc, nodeBuf, 14);
```

**Dangerous Functions\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=532
Status New

The dangerous function, memcpy, was found in use at line 479 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 571 | 571 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], unsigned *recordSize)

```
....
571.              memcpy(&attrKey, &nodeBuf[recordStart],
sizeof(attrKey));
```

**Dangerous Functions\Path 10:**

Severity Medium

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=533 |
| Status | New |

The dangerous function, memcpy, was found in use at line 479 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 595 | 595 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], unsigned *recordSize)

```
....
595.                    memcpy(&attrRec, &(nodeBuf[recordStart +
sizeof(hfsPlusAttributeKey) + attrKey.nameLength * 2]),
sizeof(attrRec));
```

**Dangerous Functions\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=534 |
| Status | New |

The dangerous function, memcpy, was found in use at line 479 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 613 | 613 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], unsigned *recordSize)

```
....
613.                    memcpy(record, &(nodeBuf[recordStart +
sizeof(hfsPlusAttributeKey) + attrKey.nameLength * 2 +
sizeof(attrRec)]), attrRec.attributeSize);
```

**Dangerous Functions\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=535 |
| Status | New |

The dangerous function, memcpy, was found in use at line 870 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 919 | 919 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
919.            memcpy(&nodeDesc, nodeBuf, 14);
```

**Dangerous Functions\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=536 |
| Status | New |

The dangerous function, memcpy, was found in use at line 870 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 981 | 981 |
| Object | memcpy | memcpy |

| | |
|---|---|
| Code Snippet | |
| File Name | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Method | static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader, |

```
....
981.                memcpy(&rectype, &(nodeBuf[recordStart + keylen + 2]),
2);
```

**Dangerous Functions\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=537 |
| Status | New |

The dangerous function, memcpy, was found in use at line 870 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 999 | 999 |
| Object | memcpy | memcpy |

| | |
|---|---|
| Code Snippet | |
| File Name | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Method | static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader, |

```
....
999.                memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

**Dangerous Functions\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=538 |
| Status | New |

The dangerous function, memcpy, was found in use at line 870 in Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1029 | 1029 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1029.                    memcpy(&header, attribute, sizeof(header));
```

**Dangerous Functions\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=539 |
| Status | New |

The dangerous function, memcpy, was found in use at line 131 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 157 | 157 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_volumeheader(cli_ctx *ctx, hfsPlusVolumeHeader **header)

```
....
157.      memcpy(volHeader, mPtr, 512);
```

**Dangerous Functions\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=540 |
| Status | New |

The dangerous function, memcpy, was found in use at line 212 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 254 | 254 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.      memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

**Dangerous Functions\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=541
Status New

The dangerous function, memcpy, was found in use at line 212 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 267 | 267 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.      memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

**Dangerous Functions\Path 19:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=542 |
| Status | New |

The dangerous function, memcpy, was found in use at line 503 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 554 | 554 |
| Object | memcpy | memcpy |

Code Snippet

File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c

Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], size_t *recordSize)

```
....
554.          memcpy(&nodeDesc, nodeBuf, 14);
```

**Dangerous Functions\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=543 |
| Status | New |

The dangerous function, memcpy, was found in use at line 503 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 596 | 596 |
| Object | memcpy | memcpy |

Code Snippet

File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c

Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], size_t *recordSize)

```
....
596.                memcpy(&attrKey, &nodeBuf[recordStart],
sizeof(attrKey));
```

**Dangerous Functions\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=544 |
| Status | New |

The dangerous function, memcpy, was found in use at line 503 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 620 | 620 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], size_t *recordSize)

```
....
620.                    memcpy(&attrRec, &(nodeBuf[recordStart +
sizeof(hfsPlusAttributeKey) + attrKey.nameLength * 2]),
sizeof(attrRec));
```

**Dangerous Functions\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=545 |
| Status | New |

The dangerous function, memcpy, was found in use at line 503 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 634 | 634 |

| | | |
|---|---|---|
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], size_t *recordSize)

```
....
634.                    memcpy(record, &(nodeBuf[recordStart +
sizeof(hfsPlusAttributeKey) + attrKey.nameLength * 2 +
sizeof(attrRec)]), attrRec.attributeSize);
```

**Dangerous Functions\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=546 |
| Status | New |

The dangerous function, memcpy, was found in use at line 919 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 972 | 972 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
972.          memcpy(&nodeDesc, nodeBuf, 14);
```

**Dangerous Functions\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=547 |
| Status | New |

The dangerous function, memcpy, was found in use at line 919 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 1034 | 1034 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1034.                memcpy(&rectype, &(nodeBuf[recordStart + keylen + 2]), 2);
```

**Dangerous Functions\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=548 |
| Status | New |

The dangerous function, memcpy, was found in use at line 919 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 1052 | 1052 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1052.                memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]), sizeof(hfsPlusCatalogFile));
```

**Dangerous Functions\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=549 |
| Status | New |

The dangerous function, memcpy, was found in use at line 919 in Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 1082 | 1082 |
| Object | memcpy | memcpy |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1082.                    memcpy(&header, attribute, sizeof(header));
```

**Dangerous Functions\Path 27:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=550
Status New

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 297 | 297 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
297.             memcpy(&lineno, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 28:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&

| | |
|---|---|
| | pathid=551 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 301 | 301 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
301.              memcpy(&tags, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=552 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 305 | 305 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
305.              memcpy(&priority, ptr, sizeof(uint8_t));
```

**Dangerous Functions\Path 30:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=553 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 309 | 309 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
309.              memcpy(&fn_size, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=554 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 331 | 331 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
331.                    memcpy(&timestamp, ptr, sizeof(struct
timespec));
```

**Dangerous Functions\Path 32:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=555 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 335 | 335 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
335.                    memcpy(&time_sec, ptr, sizeof(time_t));
```

**Dangerous Functions\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=556 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 351 | 351 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
351.                memcpy(&msg_len, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=557 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 87 | 87 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
87.    memcpy(chunk, &cs->lineno, sizeof(uint32_t));
```

**Dangerous Functions\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=558 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 91 | 91 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
91.    memcpy(chunk, &cs->tags, sizeof(uint32_t));
```

**Dangerous Functions\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=559 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 95 | 95 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
95.    memcpy(chunk, &cs->priority, sizeof(uint8_t));
```

**Dangerous Functions\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=560 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 99 | 99 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
99.    memcpy(chunk, &fn_size, sizeof(uint32_t));
```

**Dangerous Functions\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=561 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 101 | 101 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
101.        memcpy(chunk, cs->function, fn_size);
```

**Dangerous Functions\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=562 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 105 | 105 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
105.        memcpy(chunk, timestamp, sizeof(struct timespec));
```

**Dangerous Functions\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=563 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 128 | 128 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
128.        memcpy(msg_len_pt, &msg_len, sizeof(uint32_t));
```

**Dangerous Functions\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=564 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 297 | 297 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c

| | |
|---|---|
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
297.            memcpy(&lineno, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=565 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 301 | 301 |
| Object | memcpy | memcpy |

| | |
|---|---|
| Code Snippet | |
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
301.            memcpy(&tags, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=566 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 305 | 305 |
| Object | memcpy | memcpy |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
305.              memcpy(&priority, ptr, sizeof(uint8_t));
```

**Dangerous Functions\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=567 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 309 | 309 |
| Object | memcpy | memcpy |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
309.              memcpy(&fn_size, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=568 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 331 | 331 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
331.                    memcpy(&timestamp, ptr, sizeof(struct
timespec));
```

**Dangerous Functions\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=569 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 335 | 335 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
335.                    memcpy(&time_sec, ptr, sizeof(time_t));
```

**Dangerous Functions\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=570 |
| Status | New |

The dangerous function, memcpy, was found in use at line 221 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 351 | 351 |

| | | |
|---|---|---|
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
351.              memcpy(&msg_len, ptr, sizeof(uint32_t));
```

**Dangerous Functions\Path 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=571 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 87 | 87 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
87.   memcpy(chunk, &cs->lineno, sizeof(uint32_t));
```

**Dangerous Functions\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=572 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |

| | | |
|---|---|---|
| Line | 91 | 91 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
91.    memcpy(chunk, &cs->tags, sizeof(uint32_t));
```

**Dangerous Functions\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=573 |
| Status | New |

The dangerous function, memcpy, was found in use at line 55 in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c file. Such functions may expose information and allow an attacker to get full control over the host machine.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 95 | 95 |
| Object | memcpy | memcpy |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
95.    memcpy(chunk, &cs->priority, sizeof(uint8_t));
```

## 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=1000013&projectid=8&pathid=2997 |
| Status | New |

The variable declared in stream at cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c in line 157 is not initialized when it is used by stream at cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c in line 958.

| | Source | Destination |
|---|---|---|
| File | cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c | cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c |
| Line | 159 | 998 |
| Object | stream | stream |

Code Snippet
File Name cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c
Method cockpit_http_client_checkout (CockpitHttpClient *client)

```
....
159.    CockpitStream *stream = NULL;
```

File Name cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c
Method cockpit_http_stream_prepare (CockpitChannel *channel)

```
....
998.    self->stream = cockpit_http_client_checkout (self->client);
```

**Use of Zero Initialized Pointer\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2998
Status New

The variable declared in endptr at containers@@crun-0.12.1-CVE-2022-27650-TP.c in line 170 is not initialized when it is used by endptr at containers@@crun-0.12.1-CVE-2022-27650-TP.c in line 170.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.12.1-CVE-2022-27650-TP.c | containers@@crun-0.12.1-CVE-2022-27650-TP.c |
| Line | 173 | 191 |
| Object | endptr | endptr |

Code Snippet
File Name containers@@crun-0.12.1-CVE-2022-27650-TP.c
Method make_oci_process_user (const char *userspec)

```
....
173.    char *endptr = NULL;
....
191.    u->gid = strtol (endptr + 1, &endptr, 10);
```

**Use of Zero Initialized Pointer\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2999 |
| Status | New |

The variable declared in endptr at containers@@crun-0.14.1-CVE-2022-27650-TP.c in line 172 is not initialized when it is used by endptr at containers@@crun-0.14.1-CVE-2022-27650-TP.c in line 172.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.14.1-CVE-2022-27650-TP.c | containers@@crun-0.14.1-CVE-2022-27650-TP.c |
| Line | 175 | 191 |
| Object | endptr | endptr |

Code Snippet
File Name containers@@crun-0.14.1-CVE-2022-27650-TP.c
Method make_oci_process_user (const char *userspec)

```
....
175.    char *endptr = NULL;
....
191.    u->gid = strtol (endptr + 1, &endptr, 10);
```

**Use of Zero Initialized Pointer\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3000 |
| Status | New |

The variable declared in endptr at containers@@crun-0.15.1-CVE-2022-27650-TP.c in line 174 is not initialized when it is used by endptr at containers@@crun-0.15.1-CVE-2022-27650-TP.c in line 174.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.15.1-CVE-2022-27650-TP.c | containers@@crun-0.15.1-CVE-2022-27650-TP.c |
| Line | 177 | 193 |
| Object | endptr | endptr |

Code Snippet

| | |
|---|---|
| File Name | containers@@crun-0.15.1-CVE-2022-27650-TP.c |
| Method | make_oci_process_user (const char *userspec) |

```
....
177.    char *endptr = NULL;
....
193.    u->gid = strtol (endptr + 1, &endptr, 10);
```

**Use of Zero Initialized Pointer\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3001 |
| Status | New |

The variable declared in endptr at containers@@crun-0.19.1-CVE-2022-27650-TP.c in line 174 is not initialized when it is used by endptr at containers@@crun-0.19.1-CVE-2022-27650-TP.c in line 174.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.19.1-CVE-2022-27650-TP.c | containers@@crun-0.19.1-CVE-2022-27650-TP.c |
| Line | 177 | 193 |
| Object | endptr | endptr |

Code Snippet

| | |
|---|---|
| File Name | containers@@crun-0.19.1-CVE-2022-27650-TP.c |
| Method | make_oci_process_user (const char *userspec) |

```
....
177.    char *endptr = NULL;
....
193.    u->gid = strtol (endptr + 1, &endptr, 10);
```

**Use of Zero Initialized Pointer\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3002 |
| Status | New |

The variable declared in process at containers@@crun-1.4.1-CVE-2022-27650-TP.c in line 241 is not initialized when it is used by process at containers@@crun-1.4.1-CVE-2022-27650-TP.c in line 241.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-1.4.1-CVE-2022-27650-TP.c | containers@@crun-1.4.1-CVE-2022-27650-TP.c |
| Line | 247 | 278 |
| Object | process | process |

Code Snippet
File Name containers@@crun-1.4.1-CVE-2022-27650-TP.c
Method crun_command_exec (struct crun_global_arguments *global_args, int argc, char **argv, libcrun_error_t *err)

```
....
247.    cleanup_process_schema runtime_spec_schema_config_schema_process
*process = NULL;
....
278.        process = xmalloc0 (sizeof (*process));
```

**Use of Zero Initialized Pointer\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3003 |
| Status | New |

The variable declared in endptr at containers@@crun-1.4.1-CVE-2022-27650-TP.c in line 202 is not initialized when it is used by process at containers@@crun-1.4.1-CVE-2022-27650-TP.c in line 241.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-1.4.1-CVE-2022-27650-TP.c | containers@@crun-1.4.1-CVE-2022-27650-TP.c |
| Line | 205 | 291 |
| Object | endptr | process |

Code Snippet
File Name containers@@crun-1.4.1-CVE-2022-27650-TP.c
Method make_oci_process_user (const char *userspec)

```
....
205.    char *endptr = NULL;
```

File Name containers@@crun-1.4.1-CVE-2022-27650-TP.c

Method crun_command_exec (struct crun_global_arguments *global_args, int argc, char **argv, libcrun_error_t *err)

```
....
291.        process->user = make_oci_process_user (exec_options.user);
```

**Use of Zero Initialized Pointer\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3004 |
| Status | New |

The variable declared in endptr at containers@@crun-1.4.1-CVE-2022-27650-TP.c in line 202 is not initialized when it is used by endptr at containers@@crun-1.4.1-CVE-2022-27650-TP.c in line 202.

| | Source | Destination |
|---|---|---|
| File | containers@@crun-1.4.1-CVE-2022-27650-TP.c | containers@@crun-1.4.1-CVE-2022-27650-TP.c |
| Line | 205 | 221 |
| Object | endptr | endptr |

Code Snippet
File Name containers@@crun-1.4.1-CVE-2022-27650-TP.c
Method make_oci_process_user (const char *userspec)

```
....
205.    char *endptr = NULL;
....
221.    u->gid = strtol (endptr + 1, &endptr, 10);
```

**Use of Zero Initialized Pointer\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3005
Status New

The variable declared in filename at COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c in line 149 is not initialized when it is used by pFile at COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c in line 149.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c |
| Line | 157 | 164 |
| Object | filename | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
157.        const char *filename = NULL;
....
164.        pFile = fopen(filename, "r");
```

**Use of Zero Initialized Pointer\Path 10:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3006 |
| Status | New |

The variable declared in filename at COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c in line 149 is not initialized when it is used by pFile at COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c in line 149.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c |
| Line | 157 | 164 |
| Object | filename | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
157.      const char *filename = NULL;
....
164.      pFile = fopen(filename, "r");
```

**Use of Zero Initialized Pointer\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3007 |
| Status | New |

The variable declared in filename at COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c in line 158 is not initialized when it is used by pFile at COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c in line 158.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 166 | 173 |
| Object | filename | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
166.      const char *filename = NULL;
....
173.      pFile = fopen(filename, "r");
```

**Use of Zero Initialized Pointer\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3008 |
| Status | New |

The variable declared in filename at COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c in line 168 is not initialized when it is used by pFile at COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c in line 168.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 176 | 183 |
| Object | filename | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
176.      const char *filename = NULL;
....
183.      pFile = fopen(filename, "r");
```

**Use of Zero Initialized Pointer\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3009 |
| Status | New |

The variable declared in newurl at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 1511 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 2056 | 2324 |
| Object | newurl | msg |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2056.         char *newurl = NULL;
....
2324.           msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3010 |
| Status | New |

The variable declared in dns_entry at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 539 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 610 | 2324 |
| Object | dns_entry | msg |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c

Method static CURLcode multi_done(struct Curl_easy *data,

```
....
610.       conn->dns_entry = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2324.           msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3011 |
| Status | New |

The variable declared in data at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 539 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 1511.

| Source | Destination |
|---|---|

| | | |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 605 | 2324 |
| Object | data | msg |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLcode multi_done(struct Curl_easy *data,

```
....
605.    conn->data = NULL; /* the connection now has no owner */
```

File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2324.          msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 16:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3012
Status New

The variable declared in newurl at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 1511 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 1893 | 2324 |
| Object | newurl | msg |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
1893.            char *newurl = NULL;
....
2324.          msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 17:**

Severity Medium
Result State To Verify

| | |
|---|---|
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3013 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 1421 is not initialized when it is used by lstArg at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 1421.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 1446 | 1459 |
| Object | rawPath | lstArg |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_state_list(struct connectdata *conn)

```
....
1446.       char *rawPath = NULL;
....
1459.         lstArg = rawPath;
```

**Use of Zero Initialized Pointer\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3014 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 1421 is not initialized when it is used by rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 1421.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 1446 | 1455 |
| Object | rawPath | rawPath |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_state_list(struct connectdata *conn)

```
....
1446.       char *rawPath = NULL;
....
1455.         size_t n = slashPos - rawPath;
```

**Use of Zero Initialized Pointer\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3015 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 1421 is not initialized when it is used by slashPos at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 1421.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 1446 | 1451 |
| Object | rawPath | slashPos |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_state_list(struct connectdata *conn)

```
....
1446.       char *rawPath = NULL;
....
1451.       slashPos = strrchr(rawPath, '/');
```

**Use of Zero Initialized Pointer\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3016 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4086 | 4114 |
| Object | rawPath | rawPath |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.     char *rawPath = NULL; /* url-decoded "raw" path */
....
4114.           size_t dirlen = slashPos - rawPath;
```

**Use of Zero Initialized Pointer\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3017 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by fileName at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4086 | 4135 |
| Object | rawPath | fileName |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.    char *rawPath = NULL; /* url-decoded "raw" path */
....
4135.          fileName = rawPath; /* file name only (or empty) */
```

**Use of Zero Initialized Pointer\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3018 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by slashPos at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4086 | 4111 |
| Object | rawPath | slashPos |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.    char *rawPath = NULL; /* url-decoded "raw" path */
....
4111.        slashPos = strrchr(rawPath, '/');
```

**Use of Zero Initialized Pointer\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3019 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by fileName at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4086 | 4180 |
| Object | rawPath | fileName |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.    char *rawPath = NULL; /* url-decoded "raw" path */
....
4180.        fileName = curPos; /* the rest is the file name (or empty)
*/
```

**Use of Zero Initialized Pointer\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3020 |
| Status | New |

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by dirs at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4086 | 4174 |
| Object | rawPath | dirs |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.    char *rawPath = NULL; /* url-decoded "raw" path */
....
4174.              ftpc->dirs[ftpc->dirdepth++] = comp;
```

**Use of Zero Initialized Pointer\Path 25:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3021
Status New

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by fileName at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4086 | 4180 |
| Object | rawPath | fileName |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.    char *rawPath = NULL; /* url-decoded "raw" path */
....
4180.        fileName = curPos; /* the rest is the file name (or empty)
*/
```

**Use of Zero Initialized Pointer\Path 26:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3022
Status New

The variable declared in rawPath at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077 is not initialized when it is used by dirs at curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c in line 4077.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |

| | | |
|---|---|---|
| Line | 4086 | 4174 |
| Object | rawPath | dirs |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4086.    char *rawPath = NULL; /* url-decoded "raw" path */
....
4174.              ftpc->dirs[ftpc->dirdepth++] = comp;
```

**Use of Zero Initialized Pointer\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3023 |
| Status | New |

The variable declared in old_cred at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 415 is not initialized when it is used by cred at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 415.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 430 | 508 |
| Object | old_cred | cred |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
430.    struct curl_schannel_cred *old_cred = NULL;
....
508.                       BACKEND->cred->refcount));
```

**Use of Zero Initialized Pointer\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3024 |
| Status | New |

The variable declared in pCertContextServer at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 2132 is not initialized when it is used by pCertContextServer at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 2132.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 2137 | 2171 |
| Object | pCertContextServer | pCertContextServer |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method static CURLcode pkp_pin_peer_pubkey(struct connectdata *conn, int sockindex,

```
....
2137.    CERT_CONTEXT *pCertContextServer = NULL;
....
2171.      x509_der_len = pCertContextServer->cbCertEncoded;
```

**Use of Zero Initialized Pointer\Path 29:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3025
Status New

The variable declared in pCertContextServer at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 2132 is not initialized when it is used by pCertContextServer at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 2132.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 2137 | 2170 |
| Object | pCertContextServer | pCertContextServer |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method static CURLcode pkp_pin_peer_pubkey(struct connectdata *conn, int sockindex,

```
....
2137.    CERT_CONTEXT *pCertContextServer = NULL;
....
2170.      x509_der = (const char *)pCertContextServer->pbCertEncoded;
```

**Use of Zero Initialized Pointer\Path 30:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3026
Status New

The variable declared in newurl at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 1511 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 2056 | 2324 |
| Object | newurl | msg |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2056.         char *newurl = NULL;
....
2324.           msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 31:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3027
Status New

The variable declared in dns_entry at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 539 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 610 | 2324 |
| Object | dns_entry | msg |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLcode multi_done(struct Curl_easy *data,

```
....
610.       conn->dns_entry = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2324.           msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3028 |
| Status | New |

The variable declared in data at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 539 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 605 | 2324 |
| Object | data | msg |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c

Method static CURLcode multi_done(struct Curl_easy *data,

```
....
605.    conn->data = NULL; /* the connection now has no owner */
```

File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c

Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2324.           msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3029 |
| Status | New |

The variable declared in newurl at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 1511 is not initialized when it is used by msg at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 1511.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 1893 | 2324 |
| Object | newurl | msg |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Method | static CURLMcode multi_runsingle(struct Curl_multi *multi, |

```
....
1893.            char *newurl = NULL;
....
2324.          msg->extmsg.data.result = result;
```

**Use of Zero Initialized Pointer\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3030 |
| Status | New |

The variable declared in ace_hostname at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1471 is not initialized when it is used by ace_hostname at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1471.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 1490 | 1501 |
| Object | ace_hostname | ace_hostname |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Method | CURLcode Curl_idnconvert_hostname(struct connectdata *conn, |

```
....
1490.        char *ace_hostname = NULL;
....
1501.          host->encalloc = (char *)ace_hostname;
```

**Use of Zero Initialized Pointer\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3031 |
| Status | New |

The variable declared in psep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569 is not initialized when it is used by psep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 2589 | 2649 |

| | | |
|---|---|---|
| Object | psep | psep |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2589.         psep = NULL;
....
2649.         memcpy(pbuf, psep + 1, plen);
```

**Use of Zero Initialized Pointer\Path 36:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3032
Status New

The variable declared in psep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569 is not initialized when it is used by psep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 2577 | 2649 |
| Object | psep | psep |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2577.     const char *psep = NULL;
....
2649.         memcpy(pbuf, psep + 1, plen);
```

**Use of Zero Initialized Pointer\Path 37:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3033
Status New

The variable declared in osep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569 is not initialized when it is used by osep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022- | curl@@curl-curl-7_69_0-CVE-2022- |

| | | |
|---|---|---|
| | 22576-TP.c | 22576-TP.c |
| Line | 2598 | 2657 |
| Object | osep | osep |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2598.         osep = NULL;
....
2657.         memcpy(obuf, osep + 1, olen);
```

**Use of Zero Initialized Pointer\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3034 |
| Status | New |

The variable declared in osep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569 is not initialized when it is used by osep at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2569.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 2578 | 2657 |
| Object | osep | osep |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2578.     const char *osep = NULL;
....
2657.         memcpy(obuf, osep + 1, olen);
```

**Use of Zero Initialized Pointer\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3035 |
| Status | New |

The variable declared in conn_temp at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by dns_entry at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3114.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3225 |
| Object | conn_temp | dns_entry |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3225.      DEBUGASSERT(conn->dns_entry == NULL);
```

**Use of Zero Initialized Pointer\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3036 |
| Status | New |

The variable declared in endp at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 2829 is not initialized when it is used by dns_entry at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3114.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 2895 | 3225 |
| Object | endp | dns_entry |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2895.      char *endp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3225.       DEBUGASSERT(conn->dns_entry == NULL);
```

**Use of Zero Initialized Pointer\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3037 |
| Status | New |

The variable declared in Pointer at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by data at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1424.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3720 | 1426 |
| Object | Pointer | data |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3720.         *in_connect = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method void Curl_verboseconnect(struct connectdata *conn)

```
....
1426.     if(conn->data->set.verbose)
```

**Use of Zero Initialized Pointer\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3038 |
| Status | New |

The variable declared in Pointer at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by data at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1424.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |

| | | |
|---|---|---|
| Line | 3352 | 1426 |
| Object | Pointer | data |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3352.    *in_connect = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method void Curl_verboseconnect(struct connectdata *conn)

```
....
1426.    if(conn->data->set.verbose)
```

**Use of Zero Initialized Pointer\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3039 |
| Status | New |

The variable declared in conn_temp at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by data at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1424.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 1426 |
| Object | conn_temp | data |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method void Curl_verboseconnect(struct connectdata *conn)

```
....
1426.    if(conn->data->set.verbose)
```

**Use of Zero Initialized Pointer\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3040 |
| Status | New |

The variable declared in conn_temp at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3114.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3183 |
| Object | conn_temp | hostname_resolve |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode resolve_server(struct Curl_easy *data,

```
....
3183.        conn->hostname_resolve = strdup(connhost->name);
```

**Use of Zero Initialized Pointer\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3041 |
| Status | New |

The variable declared in bundle at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 186 is not initialized when it is used by bundle at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 79.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c |
| Line | 190 | 84 |
| Object | bundle | bundle |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c
Method struct connectbundle *Curl_conncache_find_bundle(struct connectdata *conn,

```
....
190.    struct connectbundle *bundle = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c

Method static void bundle_add_conn(struct connectbundle *cb_ptr,

```
....
84.    conn->bundle = cb_ptr;
```

**Use of Zero Initialized Pointer\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3042 |
| Status | New |

The variable declared in new_bundle at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 234 is not initialized when it is used by bundle at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 79.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c |
| Line | 239 | 84 |
| Object | new_bundle | bundle |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c
Method CURLcode Curl_conncache_add_conn(struct conncache *connc,

```
....
239.    struct connectbundle *new_bundle = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c

Method static void bundle_add_conn(struct connectbundle *cb_ptr,

```
....
84.    conn->bundle = cb_ptr;
```

**Use of Zero Initialized Pointer\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3043 |
| Status | New |

The variable declared in conn_candidate at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 482 is not initialized when it is used by conn_candidate at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 399.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c |
| Line | 491 | 413 |
| Object | conn_candidate | conn_candidate |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c

Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
491.    struct connectdata *conn_candidate = NULL;
```

File Name curl@@curl-curl-7_69_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 48:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3044 |
| Status | New |

The variable declared in tok_buf at curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c in line 430 is not initialized when it is used by lastc at curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c in line 430.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 782 | 1063 |
| Object | tok_buf | lastc |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c

Method Curl_cookie_add(struct Curl_easy *data,

```
....
782.       char *tok_buf = NULL;
....
1063.       lastc = clist;
```

**Use of Zero Initialized Pointer\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3045 |
| Status | New |

The variable declared in tok_buf at curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c in line 430 is not initialized when it is used by lastc at curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c in line 430.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 782 | 1057 |
| Object | tok_buf | lastc |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
782.       char *tok_buf = NULL;
....
1057.              lastc = clist;
```

**Use of Zero Initialized Pointer\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3046 |
| Status | New |

The variable declared in tok_buf at curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c in line 430 is not initialized when it is used by cookies at curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c in line 341.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 782 | 357 |
| Object | tok_buf | cookies |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Method | Curl_cookie_add(struct Curl_easy *data, |

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

| | |
|---|---|
| File Name | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Method | void Curl_cookie_loadfiles(struct Curl_easy *data) |

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

## 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=1000013&projectid=8&pathid=2587 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Line | 2562 | 2562 |
| Object | req_buffer | req_buffer |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Method | CURLcode Curl_http(struct connectdata *conn, bool *done) |

```
....
2562.     req_buffer = Curl_add_buffer_init();
```

**Memory Leak\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2588 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 1960 | 1960 |
| Object | nickname | nickname |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static CURLcode nss_setup_connect(struct connectdata *conn, int sockindex)

```
....
1960.       char *nickname = dup_nickname(data, SSL_SET_OPTION(cert));
```

**Memory Leak\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2589
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 1967 | 1967 |
| Object | nickname | nickname |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static CURLcode nss_setup_connect(struct connectdata *conn, int sockindex)

```
....
1967.       char *nickname = dup_nickname(data, SSL_SET_OPTION(cert));
```

**Memory Leak\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2590
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 1969 | 1969 |

| | | |
|---|---|---|
| Object | nickname | nickname |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static CURLcode nss_setup_connect(struct connectdata *conn, int sockindex)

```
....
1969.       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=1000013&projectid=8&pathid=2591
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 1970 | 1970 |
| Object | nickname | nickname |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static CURLcode nss_setup_connect(struct Curl_easy *data,

```
....
1970.       char *nickname = dup_nickname(data,
SSL_SET_OPTION(primary.clientcert));
```

**Memory Leak\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2592
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 87 | 87 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c

| | |
|---|---|
| Method | cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e)); |

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2593 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 99 | 99 |
| Object | e | e |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Method | cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e)); |

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2594 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 527 | 527 |
| Object | delim | delim |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Method | static void push_delimiter(subject *subj, unsigned char c, bool can_open, |

```
....
527.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2595 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 542 | 542 |
| Object | b | b |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c
Method static void push_bracket(subject *subj, bool image, cmark_node *inl_text) {

```
....
542.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2596 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 87 | 87 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2597 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 99 | 99 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2598
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 527 | 527 |
| Object | delim | delim |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method static void push_delimiter(subject *subj, unsigned char c, bool can_open,

```
....
527.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2599
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |

| | | |
|---|---|---|
| Line | 542 | 542 |
| Object | b | b |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method static void push_bracket(subject *subj, bool image, cmark_node *inl_text) {

```
....
542.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 14:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2600
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 87 | 87 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 15:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2601
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 99 | 99 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c

| | |
|---|---|
| Method | cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e)); |

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2602 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 527 | 527 |
| Object | delim | delim |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Method | static void push_delimiter(subject *subj, unsigned char c, bool can_open, |

```
....
527.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2603 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 542 | 542 |
| Object | b | b |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Method | static void push_bracket(subject *subj, bool image, cmark_node *inl_text) { |

```
....
542.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2604 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 87 | 87 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2605 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 99 | 99 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2606 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 527 | 527 |
| Object | delim | delim |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method static void push_delimiter(subject *subj, unsigned char c, bool can_open,

```
....
527.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 21:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2607
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 543 | 543 |
| Object | b | b |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method static void push_bracket(subject *subj, bool image, cmark_node *inl_text) {

```
....
543.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 22:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2608
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |

| | | |
|---|---|---|
| Line | 87 | 87 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 23:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2609
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 99 | 99 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 24:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2610
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 527 | 527 |
| Object | delim | delim |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c

| | |
|---|---|
| Method | static void push_delimiter(subject *subj, unsigned char c, bool can_open, |

```
....
527.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2611 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 543 | 543 |
| Object | b | b |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Method | static void push_bracket(subject *subj, bool image, cmark_node *inl_text) { |

```
....
543.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2612 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 87 | 87 |
| Object | e | e |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Method | cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e)); |

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2613 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 99 | 99 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2614 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 527 | 527 |
| Object | delim | delim |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method static void push_delimiter(subject *subj, unsigned char c, bool can_open,

```
....
527.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2615 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 543 | 543 |
| Object | b | b |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method static void push_bracket(subject *subj, bool image, cmark_node *inl_text) {

```
....
543.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2616 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 89 | 89 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
89.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2617 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |

| | | |
|---|---|---|
| Line | 101 | 101 |
| Object | e | e |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
101.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 32:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2618
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 531 | 531 |
| Object | delim | delim |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method static void push_delimiter(subject *subj, unsigned char c, bool can_open,

```
....
531.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 33:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2619
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 547 | 547 |
| Object | b | b |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c

| | |
|---|---|
| Method | static void push_bracket(subject *subj, bool image, cmark_node *inl_text) { |

```
....
547.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2620 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Line | 89 | 89 |
| Object | e | e |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Method | static inline cmark_node *make_literal(subject *subj, cmark_node_type t, |

```
....
89.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2621 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Line | 101 | 101 |
| Object | e | e |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Method | static inline cmark_node *make_simple(cmark_mem *mem, cmark_node_type t) { |

```
....
101.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Memory Leak\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2622 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Line | 533 | 533 |
| Object | delim | delim |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c
Method static void push_delimiter(subject *subj, unsigned char c, bool can_open,

```
....
533.    delimiter *delim = (delimiter *)subj->mem->calloc(1,
sizeof(delimiter));
```

**Memory Leak\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2623 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Line | 549 | 549 |
| Object | b | b |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c
Method static void push_bracket(subject *subj, bool image, cmark_node *inl_text) {

```
....
549.    bracket *b = (bracket *)subj->mem->calloc(1, sizeof(bracket));
```

**Memory Leak\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2624 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4168 | 4168 |
| Object | comp | comp |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4168.               char *comp = calloc(1, compLen + 1);
```

**Memory Leak\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2625 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 4168 | 4168 |
| Object | comp | comp |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4168.               char *comp = calloc(1, compLen + 1);
```

**Memory Leak\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2626 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |

| | | |
|---|---|---|
| Line | 437 | 437 |
| Object | wrap | wrap |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static CURLcode insert_wrapped_ptr(struct curl_llist *list, void *ptr)

```
....
437.    struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

**Memory Leak\Path 41:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2627
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c |
| Line | 4185 | 4185 |
| Object | comp | comp |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4185.              char *comp = calloc(1, compLen + 1);
```

**Memory Leak\Path 42:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2628
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c |
| Line | 4185 | 4185 |
| Object | comp | comp |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c

| | |
|---|---|
| Method | CURLcode ftp_parse_url_path(struct connectdata *conn) |

```
....
4185.              char *comp = calloc(1, compLen + 1);
```

**Memory Leak\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2629 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 435 | 435 |
| Object | wrap | wrap |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Method | static CURLcode insert_wrapped_ptr(struct curl_llist *list, void *ptr) |

```
....
435.    struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

**Memory Leak\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2630 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c |
| Line | 4129 | 4129 |
| Object | comp | comp |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c |
| Method | CURLcode ftp_parse_url_path(struct connectdata *conn) |

```
....
4129.              char *comp = calloc(1, compLen + 1);
```

**Memory Leak\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2631 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c |
| Line | 4129 | 4129 |
| Object | comp | comp |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8285-TP.c
Method CURLcode ftp_parse_url_path(struct connectdata *conn)

```
....
4129.              char *comp = calloc(1, compLen + 1);
```

**Memory Leak\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2632 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 435 | 435 |
| Object | wrap | wrap |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static CURLcode insert_wrapped_ptr(struct Curl_llist *list, void *ptr)

```
....
435.    struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

**Memory Leak\Path 47:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2633 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 435 | 435 |
| Object | wrap | wrap |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static CURLcode insert_wrapped_ptr(struct Curl_llist *list, void *ptr)

```
....
435.    struct ptr_list_wrap *wrap = malloc(sizeof(*wrap));
```

**Memory Leak\Path 48:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2634
Status New

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.14.1-CVE-2022-27650-TP.c | containers@@crun-0.14.1-CVE-2022-27650-TP.c |
| Line | 104 | 104 |
| Object | ret | ret |

Code Snippet
File Name containers@@crun-0.14.1-CVE-2022-27650-TP.c
Method static char **dup_array (char **arr, size_t len)

```
....
104.    ret = malloc (sizeof (char *) * (len + 1));
```

**Memory Leak\Path 49:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2635
Status New

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.15.1-CVE-2022-27650-TP.c | containers@@crun-0.15.1-CVE-2022-27650-TP.c |
| Line | 106 | 106 |

| | | |
|---|---|---|
| Object | ret | ret |

Code Snippet
File Name containers@@crun-0.15.1-CVE-2022-27650-TP.c
Method dup_array (char **arr, size_t len)

```
....
106.    ret = malloc (sizeof (char *) * (len + 1));
```

**Memory Leak\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2636 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.19.1-CVE-2022-27650-TP.c | containers@@crun-0.19.1-CVE-2022-27650-TP.c |
| Line | 106 | 106 |
| Object | ret | ret |

Code Snippet
File Name containers@@crun-0.19.1-CVE-2022-27650-TP.c
Method dup_array (char **arr, size_t len)

```
....
106.    ret = malloc (sizeof (char *) * (len + 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=1000013&projectid=8&pathid=1947 |
| Status | New |

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 1122 | 1122 |

| | | |
|---|---|---|
| Object | xmlfile | xmlfile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1122.           free(xmlfile);
```

**MemoryFree on StackVariable\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1948
Status New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 1129 | 1129 |
| Object | xmlfile | xmlfile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1129.           free(xmlfile);
```

**MemoryFree on StackVariable\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1949
Status New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 1134 | 1134 |

| | | |
|---|---|---|
| Object | xmlfile | xmlfile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1134.       free(xmlfile);
```

**MemoryFree on StackVariable\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1950
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 164 | 164 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
164.            free(dirname);
```

**MemoryFree on StackVariable\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1951
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 176 | 176 |

| | | |
|---|---|---|
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
176.              free(dirname);
```

**MemoryFree on StackVariable\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1952
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 187 | 187 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
187.          free(dirname);
```

**MemoryFree on StackVariable\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1953
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 197 | 197 |

| | | |
|---|---|---|
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
197.            free(dirname);
```

**MemoryFree on StackVariable\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1954
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 217 | 217 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
217.            free(dirname);
```

**MemoryFree on StackVariable\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1955
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 294 | 294 |

| | | |
|---|---|---|
| Object | mish_set | mish_set |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
294.                    free(mish_set);
```

**MemoryFree on StackVariable\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1956
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 299 | 299 |
| Object | mish_set | mish_set |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
299.                    free(mish_set);
```

**MemoryFree on StackVariable\Path 11:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1957
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 451 | 451 |

| | | |
|---|---|---|
| Object | mish_list_tail | mish_list_tail |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
451.          free(mish_list_tail);
```

**MemoryFree on StackVariable\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1958
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 460 | 460 |
| Object | mish_list_tail | mish_list_tail |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
460.          free(mish_list_tail);
```

**MemoryFree on StackVariable\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1959
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 464 | 464 |

| | | |
|---|---|---|
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
464.      free(dirname);
```

**MemoryFree on StackVariable\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1960 |
| Status | New |

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 494 | 494 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
494.          free(decoded);
```

**MemoryFree on StackVariable\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1961 |
| Status | New |

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 501 | 501 |

| | | |
|---|---|---|
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
501.            free(decoded);
```

**MemoryFree on StackVariable\Path 16:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1962
Status New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 509 | 509 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
509.            free(decoded);
```

**MemoryFree on StackVariable\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1963
Status New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |

| | | |
|---|---|---|
| Line | 528 | 528 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
528.            free(decoded);
```

**MemoryFree on StackVariable\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1964
Status New

Calling free() (line 1423) on a variable that was not dynamically allocated (line 1423) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1515 | 1515 |
| Object | targetdir | targetdir |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1515.       free(targetdir);
```

**MemoryFree on StackVariable\Path 19:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1965
Status New

Calling free() (line 1423) on a variable that was not dynamically allocated (line 1423) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |

| | | |
|---|---|---|
| Line | 1517 | 1517 |
| Object | volHeader | volHeader |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1517.       free(volHeader);
```

**MemoryFree on StackVariable\Path 20:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1966
Status New

Calling free() (line 317) on a variable that was not dynamically allocated (line 317) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 444 | 444 |
| Object | tmpname | tmpname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_scanfile(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *extHeader,

```
....
444.            free(tmpname);
```

**MemoryFree on StackVariable\Path 21:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1967
Status New

Calling free() (line 479) on a variable that was not dynamically allocated (line 479) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |

| | | |
|---|---|---|
| Line | 624 | 624 |
| Object | nodeBuf | nodeBuf |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_check_attribute(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *attrHeader, uint32_t expectedCnid, const uint8_t name[], uint32_t nameLen, int *found, uint8_t record[], unsigned *recordSize)

```
....
624.            free(nodeBuf);
```

**MemoryFree on StackVariable\Path 22:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1968
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 988 | 988 |
| Object | name_utf8 | name_utf8 |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
988.                        free(name_utf8);
```

**MemoryFree on StackVariable\Path 23:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1969
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1065 | 1065 |
| Object | tmpname | tmpname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1065.                                   free(tmpname);
```

**MemoryFree on StackVariable\Path 24:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1970
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1166 | 1166 |
| Object | resourceFile | resourceFile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1166.                                   free(resourceFile);
```

**MemoryFree on StackVariable\Path 25:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1971
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1294 | 1294 |
| Object | table | table |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1294.                                                   free(table);
```

**MemoryFree on StackVariable\Path 26:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1972
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1306 | 1306 |
| Object | resourceFile | resourceFile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1306.                                   free(resourceFile);
```

**MemoryFree on StackVariable\Path 27:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1973
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1340 | 1340 |
| Object | tmpname | tmpname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1340.                           free(tmpname);
```

**MemoryFree on StackVariable\Path 28:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1974
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1391 | 1391 |
| Object | name_utf8 | name_utf8 |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1391.                   free(name_utf8);
```

**MemoryFree on StackVariable\Path 29:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1975
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1411 | 1411 |
| Object | nodeBuf | nodeBuf |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1411.       free(nodeBuf);
```

**MemoryFree on StackVariable\Path 30:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1976
Status New

Calling free() (line 870) on a variable that was not dynamically allocated (line 870) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 1413 | 1413 |
| Object | name_utf8 | name_utf8 |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1413.           free(name_utf8);
```

**MemoryFree on StackVariable\Path 31:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1977
Status New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 1122 | 1122 |
| Object | xmlfile | xmlfile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1122.           free(xmlfile);
```

**MemoryFree on StackVariable\Path 32:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1978
Status New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 1129 | 1129 |
| Object | xmlfile | xmlfile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1129.           free(xmlfile);
```

**MemoryFree on StackVariable\Path 33:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1979
Status New

Calling free() (line 1096) on a variable that was not dynamically allocated (line 1096) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 1134 | 1134 |
| Object | xmlfile | xmlfile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_extract_xml(cli_ctx *ctx, char *dir, struct dmg_koly_block *hdr)

```
....
1134.       free(xmlfile);
```

**MemoryFree on StackVariable\Path 34:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1980
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 164 | 164 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
164.           free(dirname);
```

**MemoryFree on StackVariable\Path 35:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1981
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 176 | 176 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
176.              free(dirname);
```

**MemoryFree on StackVariable\Path 36:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1982
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 187 | 187 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
187.          free(dirname);
```

**MemoryFree on StackVariable\Path 37:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1983
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 197 | 197 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
197.            free(dirname);
```

**MemoryFree on StackVariable\Path 38:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1984
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 217 | 217 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
217.            free(dirname);
```

**MemoryFree on StackVariable\Path 39:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1985
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 294 | 294 |
| Object | mish_set | mish_set |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
294.                    free(mish_set);
```

**MemoryFree on StackVariable\Path 40:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1986
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 299 | 299 |
| Object | mish_set | mish_set |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
299.                    free(mish_set);
```

**MemoryFree on StackVariable\Path 41:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1987
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 451 | 451 |
| Object | mish_list_tail | mish_list_tail |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
451.          free(mish_list_tail);
```

**MemoryFree on StackVariable\Path 42:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1988
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 460 | 460 |
| Object | mish_list_tail | mish_list_tail |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
460.          free(mish_list_tail);
```

**MemoryFree on StackVariable\Path 43:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1989
Status New

Calling free() (line 95) on a variable that was not dynamically allocated (line 95) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 464 | 464 |
| Object | dirname | dirname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method int cli_scandmg(cli_ctx *ctx)

```
....
464.        free(dirname);
```

**MemoryFree on StackVariable\Path 44:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1990
Status New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 494 | 494 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
494.            free(decoded);
```

**MemoryFree on StackVariable\Path 45:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1991
Status New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 501 | 501 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
501.            free(decoded);
```

**MemoryFree on StackVariable\Path 46:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1992
Status New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 509 | 509 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
509.            free(decoded);
```

**MemoryFree on StackVariable\Path 47:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1993
Status New

Calling free() (line 472) on a variable that was not dynamically allocated (line 472) in file Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 528 | 528 |
| Object | decoded | decoded |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int dmg_decode_mish(cli_ctx *ctx, unsigned int *mishblocknum, xmlChar *mish_base64,

```
....
528.            free(decoded);
```

**MemoryFree on StackVariable\Path 48:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1994
Status New

Calling free() (line 1473) on a variable that was not dynamically allocated (line 1473) in file Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 1566 | 1566 |
| Object | targetdir | targetdir |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1566.           free(targetdir);
```

**MemoryFree on StackVariable\Path 49:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1995
Status New

Calling free() (line 1473) on a variable that was not dynamically allocated (line 1473) in file Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 1569 | 1569 |
| Object | volHeader | volHeader |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method cl_error_t cli_scanhfsplus(cli_ctx *ctx)

```
....
1569.           free(volHeader);
```

**MemoryFree on StackVariable\Path 50:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1996
Status New

Calling free() (line 317) on a variable that was not dynamically allocated (line 317) in file Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c may result with a crash.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 471 | 471 |
| Object | tmpname | tmpname |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_scanfile(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *extHeader,

```
....
471.                free(tmpname);
```

## 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=1000013&projectid=8&pathid=20 |
| Status | New |

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 254 | 254 |
| Object | hfsNodeDescriptor | hfsNodeDescriptor |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.      memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=21 |
| Status | New |

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 267 | 267 |
| Object | hfsHeaderRecord | hfsHeaderRecord |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c
Method static int hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.      memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=22 |
| Status | New |

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 870 of Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c |
| Line | 999 | 999 |
| Object | hfsPlusCatalogFile | hfsPlusCatalogFile |

Code Snippet

File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20032-TP.c

Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
999.              memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]),
sizeof(hfsPlusCatalogFile));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=23 |
| Status | New |

The size of the buffer used by hfsplus_readheader in hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsNodeDescriptor, at line 212 of Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 254 | 254 |

| | | |
|---|---|---|
| Object | hfsNodeDescriptor | hfsNodeDescriptor |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
254.      memcpy(nodeDesc, mPtr, sizeof(hfsNodeDescriptor));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=24 |
| Status | New |

The size of the buffer used by hfsplus_readheader in hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_readheader passes to hfsHeaderRecord, at line 212 of Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 267 | 267 |
| Object | hfsHeaderRecord | hfsHeaderRecord |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_readheader(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsNodeDescriptor *nodeDesc,

```
....
267.      memcpy(headerRec, mPtr + sizeof(hfsNodeDescriptor),
sizeof(hfsHeaderRecord));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=25 |
| Status | New |

The size of the buffer used by hfsplus_walk_catalog in hfsPlusCatalogFile, at line 919 of Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that hfsplus_walk_catalog passes to hfsPlusCatalogFile, at line 919 of Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c |
| Line | 1052 | 1052 |
| Object | hfsPlusCatalogFile | hfsPlusCatalogFile |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20032-TP.c
Method static cl_error_t hfsplus_walk_catalog(cli_ctx *ctx, hfsPlusVolumeHeader *volHeader, hfsHeaderRecord *catHeader,

```
....
1052.              memcpy(&fileRec, &(nodeBuf[recordStart + keylen + 2]), sizeof(hfsPlusCatalogFile));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=26
Status New

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 297 | 297 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
297.              memcpy(&lineno, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=27
Status New

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 301 | 301 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
301.              memcpy(&tags, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=28 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint8_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint8_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 305 | 305 |
| Object | uint8_t | uint8_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
305.              memcpy(&priority, ptr, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=29 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 309 | 309 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
309.              memcpy(&fn_size, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 11:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=30
Status New

The size of the buffer used by qb_log_blackbox_print_from_file in timespec, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to timespec, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 331 | 331 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
331.                    memcpy(&timestamp, ptr, sizeof(struct
timespec));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&

| | |
|---|---|
| | pathid=31 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in time_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to time_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 335 | 335 |
| Object | time_t | time_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
335.                    memcpy(&time_sec, ptr, sizeof(time_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=32 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 351 | 351 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
351.                memcpy(&msg_len, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 14:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=33 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 87 | 87 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
87.   memcpy(chunk, &cs->lineno, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=34 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 91 | 91 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
91.   memcpy(chunk, &cs->tags, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=35 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint8_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint8_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 95 | 95 |
| Object | uint8_t | uint8_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
95.    memcpy(chunk, &cs->priority, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=36 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 99 | 99 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
99.    memcpy(chunk, &fn_size, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 18:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=37 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in timespec, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to timespec, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 105 | 105 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
105.        memcpy(chunk, timestamp, sizeof(struct timespec));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=38 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 128 | 128 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
128.        memcpy(msg_len_pt, &msg_len, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=39 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 297 | 297 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
297.            memcpy(&lineno, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=40 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 301 | 301 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
301.            memcpy(&tags, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=41 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint8_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint8_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 305 | 305 |
| Object | uint8_t | uint8_t |

Code Snippet

File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c

Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
305.              memcpy(&priority, ptr, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=42 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 309 | 309 |
| Object | uint32_t | uint32_t |

Code Snippet

File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c

Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
309.              memcpy(&fn_size, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=43 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in timespec, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to timespec, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 331 | 331 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
331.                    memcpy(&timestamp, ptr, sizeof(struct
timespec));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=44 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in time_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to time_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 335 | 335 |
| Object | time_t | time_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
335.                    memcpy(&time_sec, ptr, sizeof(time_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=45 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 351 | 351 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
351.                memcpy(&msg_len, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=46 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 87 | 87 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c

| | |
|---|---|
| Method | _blackbox_vlogger(int32_t target, |

```
....
87.   memcpy(chunk, &cs->lineno, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=47 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 91 | 91 |
| Object | uint32_t | uint32_t |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | _blackbox_vlogger(int32_t target, |

```
....
91.   memcpy(chunk, &cs->tags, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=48 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint8_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint8_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 95 | 95 |
| Object | uint8_t | uint8_t |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | _blackbox_vlogger(int32_t target, |

```
....
95.    memcpy(chunk, &cs->priority, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=49 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 99 | 99 |
| Object | uint32_t | uint32_t |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | _blackbox_vlogger(int32_t target, |

```
....
99.    memcpy(chunk, &fn_size, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=50 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in timespec, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to timespec, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 105 | 105 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
105.        memcpy(chunk, timestamp, sizeof(struct timespec));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=51 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 128 | 128 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method _blackbox_vlogger(int32_t target,

```
....
128.        memcpy(msg_len_pt, &msg_len, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=52 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 297 | 297 |
| Object | uint32_t | uint32_t |

| | |
|---|---|
| Code Snippet | |
| File Name | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
297.              memcpy(&lineno, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=53 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 301 | 301 |
| Object | uint32_t | uint32_t |

| | |
|---|---|
| Code Snippet | |
| File Name | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
301.              memcpy(&tags, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=54 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint8_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint8_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 305 | 305 |

| | | |
|---|---|---|
| Object | uint8_t | uint8_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
305.              memcpy(&priority, ptr, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=55 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 309 | 309 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
309.              memcpy(&fn_size, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 37:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=56 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in timespec, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to timespec, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |

| | | |
|---|---|---|
| Line | 331 | 331 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
331.                    memcpy(&timestamp, ptr, sizeof(struct
timespec));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 38:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=57 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in time_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to time_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 335 | 335 |
| Object | time_t | time_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
335.                    memcpy(&time_sec, ptr, sizeof(time_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=58 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 351 | 351 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
351.              memcpy(&msg_len, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=59 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 87 | 87 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method _blackbox_vlogger(int32_t target,

```
....
87.   memcpy(chunk, &cs->lineno, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=60 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 91 | 91 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method _blackbox_vlogger(int32_t target,

```
....
91.    memcpy(chunk, &cs->tags, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 42:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=61
Status New

The size of the buffer used by _blackbox_vlogger in uint8_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint8_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 95 | 95 |
| Object | uint8_t | uint8_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method _blackbox_vlogger(int32_t target,

```
....
95.    memcpy(chunk, &cs->priority, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 43:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=62
Status New

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow

attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 99 | 99 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method _blackbox_vlogger(int32_t target,

```
....
99.    memcpy(chunk, &fn_size, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=63 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in timespec, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to timespec, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 105 | 105 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method _blackbox_vlogger(int32_t target,

```
....
105.        memcpy(chunk, timestamp, sizeof(struct timespec));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=64 |
| Status | New |

The size of the buffer used by _blackbox_vlogger in uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that _blackbox_vlogger passes to uint32_t, at line 55 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 128 | 128 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method _blackbox_vlogger(int32_t target,

```
....
128.        memcpy(msg_len_pt, &msg_len, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 46:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=65
Status New

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 297 | 297 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
297.            memcpy(&lineno, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 47:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=66
Status New

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 301 | 301 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
301.              memcpy(&tags, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 48:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=67
Status New

The size of the buffer used by qb_log_blackbox_print_from_file in uint8_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint8_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 305 | 305 |
| Object | uint8_t | uint8_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
305.              memcpy(&priority, ptr, sizeof(uint8_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 49:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=68

| Status | New |
|---|---|

The size of the buffer used by qb_log_blackbox_print_from_file in uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to uint32_t, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 309 | 309 |
| Object | uint32_t | uint32_t |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
309.              memcpy(&fn_size, ptr, sizeof(uint32_t));
```

**Buffer Overflow boundcpy WrongSizeParam\Path 50:**

| Severity | Medium |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=69 |
| Status | New |

The size of the buffer used by qb_log_blackbox_print_from_file in timespec, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, is not properly verified before writing data to the buffer. This can enable a buffer overflow attack, using the source buffer that qb_log_blackbox_print_from_file passes to timespec, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c, to overwrite the target buffer.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 331 | 331 |
| Object | timespec | timespec |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
331.                    memcpy(&timestamp, ptr, sizeof(struct
timespec));
```

## 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=1000013&projectid=8&pathid=322 |
| Status | New |

The function len1 in curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c at line 953 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_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 987 | 987 |
| Object | len1 | len1 |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
987.      buff1 = malloc(len1);
```

**Wrong Size t Allocation\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=323 |
| Status | New |

The function connect_idsize in curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c at line 1015 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_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 1478 | 1478 |
| Object | connect_idsize | connect_idsize |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method gtls_connect_step3(struct connectdata *conn,

```
....
1478.      connect_sessionid = malloc(connect_idsize); /* get a buffer
for it */
```

**Wrong Size t Allocation\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=324 |
| Status | New |

The function data_len in curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c at line 1465 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_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 1497 | 1497 |
| Object | data_len | data_len |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_send(struct connectdata *conn, int sockindex,

```
....
1497.    data = (unsigned char *) malloc(data_len);
```

**Wrong Size t Allocation\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=325 |
| Status | New |

The function outlen in curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c at line 682 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_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 695 | 695 |
| Object | outlen | outlen |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Method | CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data, |

```
....
695.    output = malloc(outlen);
```

**Wrong Size t Allocation\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=326 |
| Status | New |

The function pinkeylen in curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c at line 802 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_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 850 | 850 |
| Object | pinkeylen | pinkeylen |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Method | CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data, |

```
....
850.      pinkeycopy = malloc(pinkeylen);
```

**Wrong Size t Allocation\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=327 |
| Status | New |

The function new_size in curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c at line 1343 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_69_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Line | 1377 | 1377 |
| Object | new_size | new_size |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Method | CURLcode Curl_add_buffer(Curl_send_buffer **inp, const void *inptr, |

```
....
1377.        new_rb = malloc(new_size);
```

**Wrong Size t Allocation\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=328 |
| Status | New |

The function len1 in curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c at line 744 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_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 778 | 778 |
| Object | len1 | len1 |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Method | static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data, |

```
....
778.      buff1 = malloc(len1);
```

**Wrong Size t Allocation\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=329 |
| Status | New |

The function connect_idsize in curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c at line 806 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_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 1277 | 1277 |
| Object | connect_idsize | connect_idsize |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Method | gtls_connect_step3(struct connectdata *conn, |

```
....
1277.      connect_sessionid = malloc(connect_idsize); /* get a buffer
for it */
```

**Wrong Size t Allocation\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=330 |
| Status | New |

The function data_len in curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c at line 1593 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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 1625 | 1625 |
| Object | data_len | data_len |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Method | schannel_send(struct connectdata *conn, int sockindex, |

```
....
1625.    data = (unsigned char *) malloc(data_len);
```

**Wrong Size t Allocation\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=331 |
| Status | New |

The function outlen in curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c at line 711 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_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 724 | 724 |

| | | |
|---|---|---|
| Object | outlen | outlen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
724.    output = malloc(outlen);
```

**Wrong Size t Allocation\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=332 |
| Status | New |

The function pinkeylen in curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c at line 831 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_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 879 | 879 |
| Object | pinkeylen | pinkeylen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
879.      pinkeycopy = malloc(pinkeylen);
```

**Wrong Size t Allocation\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=333 |
| Status | New |

The function packetlen in curl@@curl-curl-7_71_0-CVE-2021-22945-FP.c at line 240 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_71_0-CVE-2021-22945-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22945-FP.c |

| | | |
|---|---|---|
| Line | 261 | 261 |
| Object | packetlen | packetlen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22945-FP.c
Method static CURLcode mqtt_subscribe(struct connectdata *conn)

```
....
261.    packet = malloc(packetlen);
```

**Wrong Size t Allocation\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=334 |
| Status | New |

The function len1 in curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c at line 748 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_73_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c |
| Line | 782 | 782 |
| Object | len1 | len1 |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c
Method static CURLcode pkp_pin_peer_pubkey(struct Curl_easy *data,

```
....
782.      buff1 = malloc(len1);
```

**Wrong Size t Allocation\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=335 |
| Status | New |

The function connect_idsize in curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c at line 810 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_73_0-CVE-2021- | curl@@curl-curl-7_73_0-CVE-2021- |

| | | |
|---|---|---|
| | 22890-TP.c | 22890-TP.c |
| Line | 1279 | 1279 |
| Object | connect_idsize | connect_idsize |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c
Method gtls_connect_step3(struct connectdata *conn,

```
....
1279.      connect_sessionid = malloc(connect_idsize); /* get a buffer
for it */
```

**Wrong Size t Allocation\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=336 |
| Status | New |

The function data_len in curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c at line 1600 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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 1632 | 1632 |
| Object | data_len | data_len |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_send(struct connectdata *conn, int sockindex,

```
....
1632.    data = (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=1000013&projectid=8&pathid=337 |
| Status | New |

The function outlen in curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c at line 757 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_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 770 | 770 |
| Object | outlen | outlen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
770.    output = malloc(outlen);
```

**Wrong Size t Allocation\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=338
Status New

The function pinkeylen in curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c at line 877 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_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 925 | 925 |
| Object | pinkeylen | pinkeylen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
925.      pinkeycopy = malloc(pinkeylen);
```

**Wrong Size t Allocation\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=339
Status New

The function packetlen in curl@@curl-curl-7_73_0-CVE-2021-22945-TP.c at line 242 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_73_0-CVE-2021-22945-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22945-TP.c |
| Line | 263 | 263 |
| Object | packetlen | packetlen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_subscribe(struct connectdata *conn)

```
....
263.    packet = malloc(packetlen);
```

**Wrong Size t Allocation\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=340 |
| Status | New |

The function ta_size in curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c at line 93 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_75_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c |
| Line | 189 | 189 |
| Object | ta_size | ta_size |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c
Method static CURLcode load_cafile(const char *path, br_x509_trust_anchor **anchors,

```
....
189.          ta->dn.data = malloc(ta_size);
```

**Wrong Size t Allocation\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=341 |
| Status | New |

The function data_len in curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c at line 1602 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_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 1635 | 1635 |
| Object | data_len | data_len |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_send(struct Curl_easy *data, int sockindex,

```
....
1635.    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=1000013&projectid=8&pathid=342 |
| Status | New |

The function outlen in curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c at line 763 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_75_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c |
| Line | 776 | 776 |
| Object | outlen | outlen |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
776.    output = malloc(outlen);
```

**Wrong Size t Allocation\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=343 |
| Status | New |

The function pinkeylen in curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c at line 883 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_75_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c |
| Line | 931 | 931 |
| Object | pinkeylen | pinkeylen |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
931.      pinkeycopy = malloc(pinkeylen);
```

**Wrong Size t Allocation\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=344 |
| Status | New |

The function packetlen in curl@@curl-curl-7_75_0-CVE-2021-22945-TP.c at line 246 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_75_0-CVE-2021-22945-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22945-TP.c |
| Line | 268 | 268 |
| Object | packetlen | packetlen |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_subscribe(struct Curl_easy *data)

```
....
268.    packet = malloc(packetlen);
```

**Wrong Size t Allocation\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=345 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c at line 860 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_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 917 | 917 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....
917.                                    reallocated_length);
```

**Wrong Size t Allocation\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=346 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_69_0-CVE-2021-22897-TP.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_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 1672 | 1672 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_recv(struct connectdata *conn, int sockindex,

```
....
1672.                                       reallocated_length);
```

**Wrong Size t Allocation\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=347 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_69_0-CVE-2021-22897-TP.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_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 1761 | 1761 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_recv(struct connectdata *conn, int sockindex,

```
....
1761.                                                reallocated_length);
```

**Wrong Size t Allocation\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=348 |
| Status | New |

The function newsize in curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c at line 3187 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_69_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Line | 3210 | 3210 |
| Object | newsize | newsize |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c
Method static CURLcode header_append(struct Curl_easy *data,

```
....
3210.       newbuff = realloc(data->state.headerbuff, newsize);
```

**Wrong Size t Allocation\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=349 |
| Status | New |

The function req_size in curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c at line 2446 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_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 2892 | 2892 |
| Object | req_size | req_size |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static CURLcode ossl_connect_step1(struct connectdata *conn, int sockindex)

```
....
2892.              void *tmp = realloc(enhkey_usage, req_size);
```

**Wrong Size t Allocation\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=350 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c at line 980 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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 1041 | 1041 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....
1041.                                       reallocated_length);
```

**Wrong Size t Allocation\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=351 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c at line 1735 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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 1797 | 1797 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_recv(struct connectdata *conn, int sockindex,

```
....
1797.                                          reallocated_length);
```

**Wrong Size t Allocation\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=352 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c at line 1735 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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 1886 | 1886 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_recv(struct connectdata *conn, int sockindex,

```
....
1886.                                          reallocated_length);
```

**Wrong Size t Allocation\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=353 |
| Status | New |

The function req_size in curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c at line 2452 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_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 2900 | 2900 |
| Object | req_size | req_size |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static CURLcode ossl_connect_step1(struct connectdata *conn, int sockindex)

```
....
2900.              void *tmp = realloc(enhkey_usage, req_size);
```

**Wrong Size t Allocation\Path 33:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=354
Status New

The function reallocated_length in curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c at line 983 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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 1044 | 1044 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....
1044.                                    reallocated_length);
```

**Wrong Size t Allocation\Path 34:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=355
Status New

The function reallocated_length in curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c at line 1742 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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 1804 | 1804 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_recv(struct connectdata *conn, int sockindex,

```
....
1804.                                          reallocated_length);
```

**Wrong Size t Allocation\Path 35:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=356 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c at line 1742 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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 1893 | 1893 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_recv(struct connectdata *conn, int sockindex,

```
....
1893.                                          reallocated_length);
```

**Wrong Size t Allocation\Path 36:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=357 |
| Status | New |

The function reallocated_length in curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c at line 985 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_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 1046 | 1046 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_connect_step2(struct Curl_easy *data, struct connectdata *conn,

```
....
1046.                                    reallocated_length);
```

**Wrong Size t Allocation\Path 37:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=358
Status New

The function reallocated_length in curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c at line 1745 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_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 1805 | 1805 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1805.                                    reallocated_length);
```

**Wrong Size t Allocation\Path 38:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=359
Status New

The function reallocated_length in curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c at line 1745 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_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 1894 | 1894 |
| Object | reallocated_length | reallocated_length |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_recv(struct Curl_easy *data, int sockindex,

```
....
1894.                                          reallocated_length);
```

**Wrong Size t Allocation\Path 39:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=360 |
| Status | New |

The function sslsize in curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c at line 1555 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_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 1568 | 1568 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1568.      char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 40:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=361 |
| Status | New |

The function sslsize in curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c at line 1555 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_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 1568 | 1568 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1568.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 41:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=362 |
| Status | New |

The function sslsize in curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c at line 1575 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_71_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c |
| Line | 1588 | 1588 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1588.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 42:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=363 |
| Status | New |

The function sslsize in curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c at line 1575 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_71_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c |
| Line | 1588 | 1588 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1588.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 43:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=364 |
| Status | New |

The function sslsize in curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c at line 1595 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_73_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c |
| Line | 1608 | 1608 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1608.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 44:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=365 |
| Status | New |

The function sslsize in curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c at line 1595 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_73_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c |
| Line | 1608 | 1608 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1608.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 45:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=366 |
| Status | New |

The function sslsize in curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c at line 1620 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_75_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c |
| Line | 1633 | 1633 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1633.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 46:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=367 |
| Status | New |

The function sslsize in curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c at line 1620 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_75_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c |
| Line | 1633 | 1633 |
| Object | sslsize | sslsize |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c
Method static struct connectdata *allocate_conn(struct Curl_easy *data)

```
....
1633.       char *ssl = calloc(4, sslsize);
```

**Wrong Size t Allocation\Path 47:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=368
Status New

The function len in curl@@curl-curl-7_69_0-CVE-2020-8177-TP.c at line 249 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_69_0-CVE-2020-8177-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8177-TP.c |
| Line | 257 | 257 |
| Object | len | len |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8177-TP.c
Method static char *parse_filename(const char *ptr, size_t len)

```
....
257.     copy = malloc(len + 1);
```

**Wrong Size t Allocation\Path 48:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=369
Status New

The function nread in curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c at line 2587 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_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 2771 | 2771 |
| Object | nread | nread |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_statemach_act(struct connectdata *conn)

```
....
2771.          dir = malloc(nread + 1);
```

**Wrong Size t Allocation\Path 49:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=370 |
| Status | New |

The function nread in curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c at line 2587 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_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 2864 | 2864 |
| Object | nread | nread |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_statemach_act(struct connectdata *conn)

```
....
2864.          os = malloc(nread + 1);
```

**Wrong Size t Allocation\Path 50:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=371 |
| Status | New |

The function size in curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c at line 802 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_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 918 | 918 |
| Object | size | size |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
918.      buf = malloc(size + 1);
```

## 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=1000013&projectid=8&pathid=1596
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 2185 | 2181 |
| Object | newurl | newurl |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2185.               free(newurl);
....
2181.               free(newurl);
```

**Double Free\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&

| | |
|---|---|
| | pathid=1597 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 2185 | 2181 |
| Object | newurl | newurl |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2185.               free(newurl);
....
2181.               free(newurl);
```

**Double Free\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1598 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 2623 | 2633 |
| Object | ubuf | ubuf |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2623.         free(ubuf);
....
2633.         free(ubuf);
```

**Double Free\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1599 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 254 | 254 |
| Object | per | per |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static struct per_transfer *del_per_transfer(struct per_transfer *per)

```
....
254.    free(per);
```

**Double Free\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1600
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 659 | 655 |
| Object | outfile | filename |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
659.    free(per->outfile);
....
655.      free(outs->filename);
```

**Double Free\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1601
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |

| | | |
|---|---|---|
| Line | 657 | 655 |
| Object | separator_err | filename |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
657.    free(per->separator_err);
....
655.      free(outs->filename);
```

**Double Free\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1602
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 656 | 655 |
| Object | this_url | filename |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
656.    free(per->this_url);
....
655.      free(outs->filename);
```

**Double Free\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1603
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 658 | 655 |
| Object | separator | filename |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Method | static CURLcode post_per_transfer(struct GlobalConfig *global, |

```
....
658.    free(per->separator);
....
655.      free(outs->filename);
```

**Double Free\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1604 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 2623 | 2633 |
| Object | ubuf | ubuf |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Method | CURLcode Curl_parse_login_details(const char *login, const size_t len, |

```
....
2623.        free(ubuf);
....
2633.        free(ubuf);
```

**Double Free\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1605 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |
| Line | 2342 | 2338 |
| Object | newurl | newurl |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |

| | |
|---|---|
| Method | static CURLMcode multi_runsingle(struct Curl_multi *multi, |

```
....
2342.               free(newurl);
....
2338.               free(newurl);
```

**Double Free\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1606 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Line | 2342 | 2338 |
| Object | newurl | newurl |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Method | static CURLMcode multi_runsingle(struct Curl_multi *multi, |

```
....
2342.               free(newurl);
....
2338.               free(newurl);
```

**Double Free\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1607 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c |
| Line | 2643 | 2653 |
| Object | ubuf | ubuf |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c |
| Method | CURLcode Curl_parse_login_details(const char *login, const size_t len, |

```
....
2643.         free(ubuf);
....
2653.         free(ubuf);
```

**Double Free\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1608 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 256 | 256 |
| Object | per | per |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static struct per_transfer *del_per_transfer(struct per_transfer *per)

```
....
256.     free(per);
```

**Double Free\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1609 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 660 | 658 |
| Object | separator_err | filename |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
660.    free(per->separator_err);
....
658.      free(outs->filename);
```

**Double Free\Path 15:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1610 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 659 | 658 |
| Object | this_url | filename |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
659.    free(per->this_url);
....
658.      free(outs->filename);
```

**Double Free\Path 16:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1611 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 662 | 658 |
| Object | outfile | filename |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
662.    free(per->outfile);
....
658.      free(outs->filename);
```

**Double Free\Path 17:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1612 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 661 | 658 |
| Object | separator | filename |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
661.    free(per->separator);
....
658.      free(outs->filename);
```

**Double Free\Path 18:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1613 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c |
| Line | 2643 | 2653 |
| Object | ubuf | ubuf |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2643.         free(ubuf);
....
2653.         free(ubuf);
```

**Double Free\Path 19:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1614 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c |
| Line | 2385 | 2381 |
| Object | newurl | newurl |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2385.                 free(newurl);
....
2381.                 free(newurl);
```

**Double Free\Path 20:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1615 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c |
| Line | 2678 | 2688 |
| Object | ubuf | ubuf |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2678.         free(ubuf);
....
2688.         free(ubuf);
```

**Double Free\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1616 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 256 | 256 |
| Object | per | per |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static struct per_transfer *del_per_transfer(struct per_transfer *per)

```
....
256.     free(per);
```

**Double Free\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1617 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 664 | 662 |
| Object | separator_err | filename |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
664.    free(per->separator_err);
....
662.      free(outs->filename);
```

**Double Free\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1618 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 663 | 662 |
| Object | this_url | filename |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
663.    free(per->this_url);
....
662.      free(outs->filename);
```

**Double Free\Path 24:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1619 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 666 | 662 |
| Object | outfile | filename |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
666.    free(per->outfile);
....
662.      free(outs->filename);
```

**Double Free\Path 25:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1620 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 665 | 662 |
| Object | separator | filename |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
665.    free(per->separator);
....
662.      free(outs->filename);
```

**Double Free\Path 26:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1621 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c |
| Line | 2678 | 2688 |
| Object | ubuf | ubuf |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2678.         free(ubuf);
....
2688.         free(ubuf);
```

**Double Free\Path 27:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1622 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22901-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22901-TP.c |
| Line | 2246 | 2242 |
| Object | newurl | newurl |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22901-TP.c
Method static CURLMcode multi_runsingle(struct Curl_multi *multi,

```
....
2246.                 free(newurl);
....
2242.                 free(newurl);
```

**Double Free\Path 28:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1623 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c |
| Line | 2736 | 2746 |
| Object | ubuf | ubuf |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2736.         free(ubuf);
....
2746.         free(ubuf);
```

**Double Free\Path 29:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1624 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 256 | 256 |
| Object | per | per |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static struct per_transfer *del_per_transfer(struct per_transfer *per)

```
....
256.     free(per);
```

**Double Free\Path 30:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1625 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 667 | 665 |
| Object | separator_err | filename |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
667.    free(per->separator_err);
....
665.      free(outs->filename);
```

**Double Free\Path 31:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1626 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 666 | 665 |
| Object | this_url | filename |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
666.    free(per->this_url);
....
665.      free(outs->filename);
```

**Double Free\Path 32:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1627 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 669 | 665 |
| Object | outfile | filename |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
669.    free(per->outfile);
....
665.      free(outs->filename);
```

**Double Free\Path 33:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1628 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 668 | 665 |
| Object | separator | filename |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode post_per_transfer(struct GlobalConfig *global,

```
....
668.    free(per->separator);
....
665.      free(outs->filename);
```

**Double Free\Path 34:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1629 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c |
| Line | 2736 | 2746 |
| Object | ubuf | ubuf |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c
Method CURLcode Curl_parse_login_details(const char *login, const size_t len,

```
....
2736.         free(ubuf);
....
2746.         free(ubuf);
```

## 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=1000013&projectid=8&pathid=501 |
| 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_69_0-CVE-2020-8231-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_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 1092 | 1092 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode Curl_multi_wait(struct Curl_multi *multi,

```
....
1092.       timeout_ms = (int)timeout_internal;
```

**Integer Overflow\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=502 |
| 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_69_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_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 1092 | 1092 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode Curl_multi_wait(struct Curl_multi *multi,

```
....
1092.       timeout_ms = (int)timeout_internal;
```

**Integer Overflow\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=503
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2829 of curl@@curl-curl-7_69_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_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 2907 | 2907 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2907.           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=1000013&projectid=8&pathid=504
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2829 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 2907 | 2907 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2907.          port = (int)portparse; /* we know it will fit */
```

**Integer Overflow\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=505
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 856 of curl@@curl-curl-7_69_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_69_0-CVE-2023-28320-TP.c | curl@@curl-curl-7_69_0-CVE-2023-28320-TP.c |
| Line | 920 | 920 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
920.        port = (int)tmp_port;
```

**Integer Overflow\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=506
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1062 of curl@@curl-curl-7_71_0-CVE-2020-8231-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_71_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |
| Line | 1124 | 1124 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c
Method static CURLMcode Curl_multi_wait(struct Curl_multi *multi,

```
....
1124.       timeout_ms = (int)timeout_internal;
```

**Integer Overflow\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=507
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3359 of curl@@curl-curl-7_71_0-CVE-2020-8286-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_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 3363 | 3363 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static int asn1_object_dump(ASN1_OBJECT *a, char *buf, size_t len)

```
....
3363.     ilen = (int)len;
```

**Integer Overflow\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=508
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4102 of curl@@curl-curl-7_71_0-CVE-2020-8286-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_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 4120 | 4120 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_send(struct connectdata *conn,

```
....
4120.    memlen = (len > (size_t)INT_MAX) ? INT_MAX : (int)len;
```

**Integer Overflow\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=509
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4183 of curl@@curl-curl-7_71_0-CVE-2020-8286-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_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 4198 | 4198 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_recv(struct connectdata *conn, /* connection data */

```
....
4198.    buffsize = (buffersize > (size_t)INT_MAX) ? INT_MAX :
(int)buffersize;
```

**Integer Overflow\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=510
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1062 of curl@@curl-curl-7_71_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_71_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Line | 1124 | 1124 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c
Method static CURLMcode Curl_multi_wait(struct Curl_multi *multi,

```
....
1124.       timeout_ms = (int)timeout_internal;
```

**Integer Overflow\Path 11:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=511
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2851 of curl@@curl-curl-7_71_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_71_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c |
| Line | 2929 | 2929 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2929.           port = (int)portparse; /* we know it will fit */
```

**Integer Overflow\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=512
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2851 of curl@@curl-curl-7_71_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_71_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c |
| Line | 2929 | 2929 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2929.           port = (int)portparse; /* we know it will fit */
```

**Integer Overflow\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=513
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 872 of curl@@curl-curl-7_71_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_71_0-CVE-2023-28320-TP.c | curl@@curl-curl-7_71_0-CVE-2023-28320-TP.c |
| Line | 936 | 936 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
936.        port = (int)tmp_port;
```

**Integer Overflow\Path 14:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=514
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 3357 of curl@@curl-curl-7_73_0-CVE-2020-8286-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_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 3361 | 3361 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static int asn1_object_dump(ASN1_OBJECT *a, char *buf, size_t len)

```
....
3361.    ilen = (int)len;
```

**Integer Overflow\Path 15:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=515
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4094 of curl@@curl-curl-7_73_0-CVE-2020-8286-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_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 4112 | 4112 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_send(struct connectdata *conn,

```
....
4112.    memlen = (len > (size_t)INT_MAX) ? INT_MAX : (int)len;
```

**Integer Overflow\Path 16:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=516
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 4175 of curl@@curl-curl-7_73_0-CVE-2020-8286-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_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 4190 | 4190 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_recv(struct connectdata *conn, /* connection data */

```
....
4190.    buffsize = (buffersize > (size_t)INT_MAX) ? INT_MAX :
(int)buffersize;
```

**Integer Overflow\Path 17:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=517
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1076 of curl@@curl-curl-7_73_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_73_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c |
| Line | 1140 | 1140 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c
Method static CURLMcode Curl_multi_wait(struct Curl_multi *multi,

```
....
1140.      timeout_ms = (int)timeout_internal;
```

**Integer Overflow\Path 18:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=518
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2886 of curl@@curl-curl-7_73_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_73_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c |
| Line | 2964 | 2964 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2964.          port = (int)portparse; /* we know it will fit */
```

**Integer Overflow\Path 19:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=519
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2886 of curl@@curl-curl-7_73_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_73_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c |
| Line | 2964 | 2964 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
2964.          port = (int)portparse; /* we know it will fit */
```

**Integer Overflow\Path 20:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=520
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 872 of curl@@curl-curl-7_73_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_73_0-CVE-2023-28320-TP.c | curl@@curl-curl-7_73_0-CVE-2023-28320-TP.c |
| Line | 936 | 936 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2023-28320-TP.c
Method CURLcode Curl_loadhostpairs(struct Curl_easy *data)

```
....
936.         port = (int)tmp_port;
```

**Integer Overflow\Path 21:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=521 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 1077 of curl@@curl-curl-7_75_0-CVE-2021-22901-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-2021-22901-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22901-TP.c |
| Line | 1135 | 1135 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22901-TP.c
Method static CURLMcode multi_wait(struct Curl_multi *multi,

```
....
1135.       timeout_ms = (int)timeout_internal;
```

**Integer Overflow\Path 22:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=522 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2944 of curl@@curl-curl-7_75_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_75_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c |
| Line | 3022 | 3022 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3022.           port = (int)portparse; /* we know it will fit */
```

**Integer Overflow\Path 23:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=523 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 2944 of curl@@curl-curl-7_75_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_75_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c |
| Line | 3022 | 3022 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c
Method static CURLcode parse_connect_to_host_port(struct Curl_easy *data,

```
....
3022.           port = (int)portparse; /* we know it will fit */
```

## 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=1000013&projectid=8&pathid=1643 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c |
| Line | 436 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
436.                    curlx_uztoui(strlen(conn->passwd)));
....
435.    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=1000013&projectid=8&pathid=1644 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c |
| Line | 435 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
435.    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=1000013&projectid=8&pathid=1645 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c |
| Line | 436 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
436.                    curlx_uztoui(strlen(conn->passwd)));
....
435.    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=1000013&projectid=8&pathid=1646 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c |
| Line | 435 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
435.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1647 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c |
| Line | 436 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
436.                    curlx_uztoui(strlen(conn->passwd)));
....
435.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1648 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c |
| Line | 435 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
435.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1649 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c |
| Line | 436 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
436.                    curlx_uztoui(strlen(conn->passwd)));
....
435.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1650 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 410 of curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c at line 410.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c |
| Line | 435 | 435 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
435.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 9:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1651 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 412 of curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c at line 412.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c |
| Line | 438 | 437 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
438.                    curlx_uztoui(strlen(conn->passwd)));
....
437.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 10:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1652 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 412 of curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c at line 412.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c |
| Line | 437 | 437 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22946-TP.c

| | |
|---|---|
| Method | static CURLcode pop3_perform_apop(struct connectdata *conn) |

```
....
437.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 11:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1653 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 412 of curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c at line 412.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c |
| Line | 438 | 437 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct connectdata *conn)

```
....
438.                    curlx_uztoui(strlen(conn->passwd)));
....
437.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 12:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1654 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 412 of curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c at line 412.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c |
| Line | 437 | 437 |
| Object | passwd | Curl_MD5_update |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_73_0-CVE-2021-22947-TP.c |
| Method | static CURLcode pop3_perform_apop(struct connectdata *conn) |

```
....
437.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 13:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1655 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 422 of curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c at line 422.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c |
| Line | 449 | 448 |
| Object | passwd | Curl_MD5_update |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c |
| Method | static CURLcode pop3_perform_apop(struct Curl_easy *data, |

```
....
449.                    curlx_uztoui(strlen(conn->passwd)));
....
448.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

**Inadequate Encryption Strength\Path 14:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1656 |
| Status | New |

The application uses a weak cryptographic algorithm, Curl_MD5_update at line 422 of curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c, to protect sensitive personal information passwd, from curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c at line 422.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c |
| Line | 448 | 448 |
| Object | passwd | Curl_MD5_update |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22947-TP.c
Method static CURLcode pop3_perform_apop(struct Curl_easy *data,

```
....
448.    Curl_MD5_update(ctxt, (const unsigned char *) conn->passwd,
```

## 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=1000013&projectid=8&pathid=1630 |
| Status | New |

Method ssl_ui_reader at line 510 of curl@@curl-curl-7_71_0-CVE-2020-8286-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_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 512 | 512 |
| Object | password | password |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static int ssl_ui_reader(UI *ui, UI_STRING *uis)

```
....
512.    const char *password;
```

**Heap Inspection\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1631 |
| Status | New |

Method schannel_connect_step1 at line 406 of curl@@curl-curl-7_71_0-CVE-2021-22897-TP.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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 642 | 642 |
| Object | pszPassword | pszPassword |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
642.          WCHAR* pszPassword;
```

**Heap Inspection\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1632
Status New

Method ssl_ui_reader at line 522 of curl@@curl-curl-7_73_0-CVE-2020-8286-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_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 524 | 524 |
| Object | password | password |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static int ssl_ui_reader(UI *ui, UI_STRING *uis)

```
....
524.    const char *password;
```

**Heap Inspection\Path 4:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1633
Status New

Method schannel_connect_step1 at line 408 of curl@@curl-curl-7_73_0-CVE-2021-22897-TP.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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 645 | 645 |
| Object | pszPassword | pszPassword |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
645.          WCHAR* pszPassword;
```

**Heap Inspection\Path 5:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1634
Status New

Method schannel_connect_step1 at line 409 of curl@@curl-curl-7_75_0-CVE-2021-22897-TP.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_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 647 | 647 |
| Object | pszPassword | pszPassword |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
647.          WCHAR* pszPassword;
```

**Heap Inspection\Path 6:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1635
Status New

Method http_output_basic at line 283 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Line | 290 | 290 |
| Object | pwd | pwd |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c
Method static CURLcode http_output_basic(struct connectdata *conn, bool proxy)

```
....
290.    const char *pwd;
```

**Heap Inspection\Path 7:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1636
Status New

Method http_output_basic at line 283 of curl@@curl-curl-7_71_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_71_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27776-TP.c |
| Line | 290 | 290 |
| Object | pwd | pwd |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27776-TP.c
Method static CURLcode http_output_basic(struct connectdata *conn, bool proxy)

```
....
290.    const char *pwd;
```

**Heap Inspection\Path 8:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1637
Status New

Method http_output_basic at line 287 of curl@@curl-curl-7_73_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_73_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27776-TP.c |
| Line | 294 | 294 |
| Object | pwd | pwd |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27776-TP.c
Method static CURLcode http_output_basic(struct connectdata *conn, bool proxy)

```
....
294.    const char *pwd;
```

**Heap Inspection\Path 9:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1638
Status New

Method http_output_basic at line 297 of curl@@curl-curl-7_75_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_75_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27776-TP.c |
| Line | 304 | 304 |
| Object | pwd | pwd |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27776-TP.c
Method static CURLcode http_output_basic(struct Curl_easy *data, bool proxy)

```
....
304.    const char *pwd;
```

**Heap Inspection\Path 10:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1639
Status New

Method schannel_connect_step1 at line 406 of curl@@curl-curl-7_71_0-CVE-2021-22897-TP.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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 643 | 643 |
| Object | pwd_len | pwd_len |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
643.          size_t pwd_len = 0;
```

**Heap Inspection\Path 11:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1640
Status New

Method schannel_connect_step1 at line 408 of curl@@curl-curl-7_73_0-CVE-2021-22897-TP.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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 646 | 646 |
| Object | pwd_len | pwd_len |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
646.          size_t pwd_len = 0;
```

**Heap Inspection\Path 12:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1641
Status New

Method schannel_connect_step1 at line 409 of curl@@curl-curl-7_75_0-CVE-2021-22897-TP.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_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 648 | 648 |
| Object | pwd_len | pwd_len |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
648.          size_t pwd_len = 0;
```

**Heap Inspection\Path 13:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1642
Status New

Method imap_perform_login at line 498 of curl@@curl-curl-7_75_0-CVE-2021-22946-TP.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_75_0-CVE-2021-22946-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22946-TP.c |
| Line | 503 | 503 |
| Object | passwd | passwd |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22946-TP.c
Method static CURLcode imap_perform_login(struct Curl_easy *data,

```
....
503.    char *passwd;
```

## 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=1000013&projectid=8&pathid=487 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 946 of curl@@curl-curl-7_69_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_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 965 | 965 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
965.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=488 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 946 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 965 | 965 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
965.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=489 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 940 of curl@@curl-curl-7_71_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_71_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c |
| Line | 959 | 959 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-22576-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
959.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=490 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 940 of curl@@curl-curl-7_71_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_71_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c |
| Line | 959 | 959 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
959.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=491 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 954 of curl@@curl-curl-7_73_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_73_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c |
| Line | 973 | 973 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-22576-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
973.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=492 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 954 of curl@@curl-curl-7_73_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_73_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c |
| Line | 973 | 973 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
973.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 7:**

| | |
|---|---|
| Severity | Medium |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=493 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 969 of curl@@curl-curl-7_75_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_75_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c |
| Line | 991 | 991 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-22576-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
991.        dead = (state & CONNRESULT_DEAD);
```

**Boolean Overflow\Path 8:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=494 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 969 of curl@@curl-curl-7_75_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_75_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c |
| Line | 991 | 991 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27782-TP.c
Method static bool extract_if_dead(struct connectdata *conn,

```
....
991.        dead = (state & CONNRESULT_DEAD);
```

## Buffer Overflow AddressOfLocalVarReturned

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

## Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SC-5 Denial of Service Protection (P1)
OWASP Top 10 2017: A1-Injection

## *Description*

**Buffer Overflow AddressOfLocalVarReturned\Path 1:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=13 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c |
| Line | 544 | 544 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.103.7-CVE-2023-20052-TP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.      return a->startSector - b->startSector;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=14 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c in line 541 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c |
| Line | 544 | 544 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-0.105.0-rc-CVE-2023-20052-TP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.      return a->startSector - b->startSector;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=15 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20052-TP.c in line 542 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20052-TP.c | Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20052-TP.c |
| Line | 545 | 545 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.0-rc2-CVE-2023-20052-TP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
545.      return a->startSector - b->startSector;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=16 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-1.0.1-CVE-2023-20052-FP.c in line 541 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.0.1-CVE-2023-20052-FP.c | Cisco-Talos@@clamav-clamav-1.0.1-CVE-2023-20052-FP.c |
| Line | 544 | 544 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.0.1-CVE-2023-20052-FP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.      return a->startSector - b->startSector;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=17 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-1.2.0-rc-CVE-2023-20052-FP.c in line 541 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.2.0-rc-CVE-2023-20052-FP.c | Cisco-Talos@@clamav-clamav-1.2.0-rc-CVE-2023-20052-FP.c |
| Line | 544 | 544 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.2.0-rc-CVE-2023-20052-FP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.      return a->startSector - b->startSector;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=18 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-1.3.0-rc-CVE-2023-20052-FP.c in line 541 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.3.0-rc-CVE-2023-20052-FP.c | Cisco-Talos@@clamav-clamav-1.3.0-rc-CVE-2023-20052-FP.c |
| Line | 544 | 544 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.3.0-rc-CVE-2023-20052-FP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
544.      return a->startSector - b->startSector;
```

**Buffer Overflow AddressOfLocalVarReturned\Path 7:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=19 |
| Status | New |

The pointer b at Cisco-Talos@@clamav-clamav-1.4.0-rc-CVE-2023-20052-FP.c in line 520 is being used after it has been freed.

| | Source | Destination |
|---|---|---|
| File | Cisco-Talos@@clamav-clamav-1.4.0-rc-CVE-2023-20052-FP.c | Cisco-Talos@@clamav-clamav-1.4.0-rc-CVE-2023-20052-FP.c |
| Line | 523 | 523 |
| Object | b | b |

Code Snippet
File Name Cisco-Talos@@clamav-clamav-1.4.0-rc-CVE-2023-20052-FP.c
Method static int cmp_mish_stripes(const void *stripe_a, const void *stripe_b)

```
....
523.      return a->startSector - b->startSector;
```

## 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=1000013&projectid=8&pathid=495 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 139 of curl@@curl-curl-7_71_0-CVE-2021-22945-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_71_0-CVE-2021- | curl@@curl-curl-7_71_0-CVE-2021- |

| | | |
|---|---|---|
| | 22945-FP.c | 22945-FP.c |
| Line | 156 | 156 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22945-FP.c
Method static CURLcode mqtt_connect(struct connectdata *conn)

```
....
156.    packet[1] = (packetlen - 2) & 0x7f;
```

**Char Overflow\Path 2:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=496
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 224 of curl@@curl-curl-7_71_0-CVE-2021-22945-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_71_0-CVE-2021-22945-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22945-FP.c |
| Line | 230 | 230 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22945-FP.c
Method static int mqtt_encode_len(char *buf, size_t len)

```
....
230.      encoded = len % 0x80;
```

**Char Overflow\Path 3:**

Severity Medium
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=497
Status New

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 140 of curl@@curl-curl-7_73_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_73_0-CVE-2021- | curl@@curl-curl-7_73_0-CVE-2021- |

| | | |
|---|---|---|
| | 22945-TP.c | 22945-TP.c |
| Line | 157 | 157 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_connect(struct connectdata *conn)

```
....
157.    packet[1] = (packetlen - 2) & 0x7f;
```

**Char Overflow\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=498 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 226 of curl@@curl-curl-7_73_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_73_0-CVE-2021-22945-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22945-TP.c |
| Line | 232 | 232 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22945-TP.c
Method static int mqtt_encode_len(char *buf, size_t len)

```
....
232.      encoded = len % 0x80;
```

**Char Overflow\Path 5:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=499 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 145 of curl@@curl-curl-7_75_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_75_0-CVE-2021- | curl@@curl-curl-7_75_0-CVE-2021- |

| | | |
|---|---|---|
| | 22945-TP.c | 22945-TP.c |
| Line | 162 | 162 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22945-TP.c
Method static CURLcode mqtt_connect(struct Curl_easy *data)

```
....
162.    packet[1] = (packetlen - 2) & 0x7f;
```

**Char Overflow\Path 6:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=500 |
| Status | New |

A variable of a larger data type, AssignExpr, is being assigned to a smaller data type, in 230 of curl@@curl-curl-7_75_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_75_0-CVE-2021-22945-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22945-TP.c |
| Line | 236 | 236 |
| Object | AssignExpr | AssignExpr |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22945-TP.c
Method static int mqtt_encode_len(char *buf, size_t len)

```
....
236.      encoded = len % 0x80;
```

## Off by One Error in Methods

Query Path:
CPP\Cx\CPP Buffer Overflow\Off by One Error in Methods Version:0

### Categories

PCI DSS v3.2: PCI DSS (3.2) - 6.5.2 - Buffer overflows
NIST SP 800-53: SI-16 Memory Protection (P1)
OWASP Top 10 2017: A1-Injection

*Description*

**Off by One Error in Methods\Path 1:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=318 |
| Status | New |

The buffer allocated by sizeof in curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c at line 4102 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 4143 | 4143 |
| Object | error_buffer | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_send(struct connectdata *conn,

```
....
4143.            strncpy(error_buffer, SSL_ERROR_to_str(err),
sizeof(error_buffer));
```

**Off by One Error in Methods\Path 2:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=319 |
| Status | New |

The buffer allocated by sizeof in curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c at line 4183 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 4233 | 4233 |
| Object | error_buffer | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_recv(struct connectdata *conn, /* connection data */

```
....
4233.            strncpy(error_buffer, SSL_ERROR_to_str(err),
sizeof(error_buffer));
```

**Off by One Error in Methods\Path 3:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=320 |
| Status | New |

The buffer allocated by sizeof in curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c at line 4094 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 4135 | 4135 |
| Object | error_buffer | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_send(struct connectdata *conn,

```
....
4135.            strncpy(error_buffer, SSL_ERROR_to_str(err),
sizeof(error_buffer));
```

**Off by One Error in Methods\Path 4:**

| | |
|---|---|
| Severity | Medium |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=321 |
| Status | New |

The buffer allocated by sizeof in curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c at line 4175 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 4225 | 4225 |
| Object | error_buffer | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method static ssize_t ossl_recv(struct connectdata *conn, /* connection data */

```
....
4225.            strncpy(error_buffer, SSL_ERROR_to_str(err),
sizeof(error_buffer));
```

## Improper Resource Access Authorization

Query Path:

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=1000013&projectid=8&pathid=3585 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c |
| Line | 169 | 169 |
| Object | fgets | fgets |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3586 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c |
| Line | 169 | 169 |
| Object | fgets | fgets |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3587 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 178 | 178 |
| Object | fgets | fgets |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
178.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3588 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 188 | 188 |
| Object | fgets | fgets |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
188.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3589 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c |
| Line | 169 | 169 |
| Object | line | line |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 6:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3590 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c |
| Line | 169 | 169 |
| Object | line | line |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
169.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 7:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3591 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |

| | | |
|---|---|---|
| Line | 178 | 178 |
| Object | line | line |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
178.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3592
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 188 | 188 |
| Object | line | line |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
188.                if (fgets(line, value_length - 1, pFile) != NULL) {
```

**Improper Resource Access Authorization\Path 9:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3593
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c |
| Line | 543 | 543 |
| Object | buffer | buffer |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c

| | |
|---|---|
| Method | cmark_node *cmark_parse_file(FILE *f, int options) { |

```
....
543.    while ((bytes = fread(buffer, 1, sizeof(buffer), f)) > 0) {
```

**Improper Resource Access Authorization\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3594 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Line | 543 | 543 |
| Object | buffer | buffer |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Method | cmark_node *cmark_parse_file(FILE *f, int options) { |

```
....
543.    while ((bytes = fread(buffer, 1, sizeof(buffer), f)) > 0) {
```

**Improper Resource Access Authorization\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3595 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c |
| Line | 543 | 543 |
| Object | buffer | buffer |

| | |
|---|---|
| Code Snippet | |
| File Name | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c |
| Method | cmark_node *cmark_parse_file(FILE *f, int options) { |

```
....
543.    while ((bytes = fread(buffer, 1, sizeof(buffer), f)) > 0) {
```

**Improper Resource Access Authorization\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3596 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c |
| Line | 546 | 546 |
| Object | buffer | buffer |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c
Method cmark_node *cmark_parse_file(FILE *f, int options) {

```
....
546.    while ((bytes = fread(buffer, 1, sizeof(buffer), f)) > 0) {
```

**Improper Resource Access Authorization\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3597 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 687 | 687 |
| Object | buffer | buffer |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
687.        if (fread(buffer, sizeof(buffer), 1, handle) != 0) {
```

**Improper Resource Access Authorization\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3598 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 683 | 683 |
| Object | buffer | buffer |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
683.      if (fread(buffer, sizeof(buffer), 1, handle) != 0) {
```

**Improper Resource Access Authorization\Path 15:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3599
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 261 | 261 |
| Object | ptr | ptr |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
261.    if(fread(ptr, 1, (size_t)filelen, f) < (size_t)filelen) {
```

**Improper Resource Access Authorization\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3600
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |

| | | |
|---|---|---|
| Line | 923 | 923 |
| Object | buf | buf |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
923.      if((int) fread(buf, size, 1, fp) != 1)
```

**Improper Resource Access Authorization\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3601
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 173 | 173 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_69_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 18:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3602
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 184 | 184 |
| Object | ptr | ptr |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c

| | |
|---|---|
| Method | static gnutls_datum_t load_file(const char *file) |

```
....
184.    if(fread(ptr, 1, (size_t)filelen, f) < (size_t)filelen) {
```

**Improper Resource Access Authorization\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3603 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 662 | 662 |
| Object | certdata | certdata |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Method | schannel_connect_step1(struct connectdata *conn, int sockindex) |

```
....
662.                ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

**Improper Resource Access Authorization\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3604 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 952 | 952 |
| Object | buf | buf |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Method | CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data, |

```
....
952.      if((int) fread(buf, size, 1, fp) != 1)
```

**Improper Resource Access Authorization\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3605 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 175 | 175 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_71_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 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3606 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 1578 | 1578 |
| Object | certdata | certdata |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1578.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

**Improper Resource Access Authorization\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3607 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 1621 | 1621 |
| Object | certdata | certdata |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1621.                   ((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=1000013&projectid=8&pathid=3608
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c |
| Line | 184 | 184 |
| Object | ptr | ptr |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
184.    if(fread(ptr, 1, (size_t)filelen, f) < (size_t)filelen) {
```

**Improper Resource Access Authorization\Path 25:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3609
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |

| | | |
|---|---|---|
| Line | 665 | 665 |
| Object | certdata | certdata |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
665.                ((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=1000013&projectid=8&pathid=3610
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 998 | 998 |
| Object | buf | buf |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
998.      if((int) fread(buf, size, 1, fp) != 1)
```

**Improper Resource Access Authorization\Path 27:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3611
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 175 | 175 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_73_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 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3612 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1594 | 1594 |
| Object | certdata | certdata |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
1594.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

**Improper Resource Access Authorization\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3613 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1637 | 1637 |
| Object | certdata | certdata |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
1637.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

**Improper Resource Access Authorization\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3614 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c |
| Line | 119 | 119 |
| Object | buf | buf |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c
Method static CURLcode load_cafile(const char *path, br_x509_trust_anchor **anchors,

```
....
119.      n = fread(buf, 1, sizeof(buf), fp);
```

**Improper Resource Access Authorization\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3615 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 667 | 667 |
| Object | certdata | certdata |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
667.              ((int) fread(certdata, certsize, 1, fInCert) != 1))
```

**Improper Resource Access Authorization\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3616 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c |
| Line | 1004 | 1004 |
| Object | buf | buf |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
1004.       if((int) fread(buf, size, 1, fp) != 1)
```

**Improper Resource Access Authorization\Path 33:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3617 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 175 | 175 |
| Object | buffer | buffer |

Code Snippet
File Name curl@@curl-curl-7_75_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 34:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3618 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |

| | | |
|---|---|---|
| Line | 1598 | 1598 |
| Object | certdata | certdata |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1598.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

**Improper Resource Access Authorization\Path 35:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3619
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 1641 | 1641 |
| Object | certdata | certdata |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1641.                   ((int)fread(certdata, (size_t)filesize, 1,
fInCert) != 1))
```

**Improper Resource Access Authorization\Path 36:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3620
Status New

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 243 | 243 |
| Object | Address | Address |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
243.        err = read(fd, &header, sizeof(header));
```

**Improper Resource Access Authorization\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3621 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 243 | 243 |
| Object | Address | Address |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
243.        err = read(fd, &header, sizeof(header));
```

**Improper Resource Access Authorization\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3622 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 243 | 243 |
| Object | Address | Address |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
243.        err = read(fd, &header, sizeof(header));
```

**Improper Resource Access Authorization\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3623 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 243 | 243 |
| Object | Address | Address |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
243.        err = read(fd, &header, sizeof(header));
```

**Improper Resource Access Authorization\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3624 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c |
| Line | 243 | 243 |
| Object | Address | Address |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
243.        err = read(fd, &header, sizeof(header));
```

**Improper Resource Access Authorization\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3625 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c |
| Line | 242 | 242 |
| Object | Address | Address |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
242.        err = read(fd, &header, sizeof(header));
```

**Improper Resource Access Authorization\Path 42:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3626
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 303 | 303 |
| Object | fprintf | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
303.                    fprintf (stderr, "Option -%c requires an
argument.\n", optopt);
```

**Improper Resource Access Authorization\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3627
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |

| | | |
|---|---|---|
| Line | 305 | 305 |
| Object | fprintf | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
305.                    fprintf (stderr, "Unknown option `-%c'.\n",
optopt);
```

**Improper Resource Access Authorization\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3628
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 307 | 307 |
| Object | fprintf | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
307.                    fprintf (stderr, "Unknown option character
`\\x%x'.\n", optopt);
```

**Improper Resource Access Authorization\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3629
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 338 | 338 |
| Object | fprintf | fprintf |

Code Snippet

| | |
|---|---|
| File Name | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Method | int main(int argc, char *argv[]) |

```
....
338.              fprintf(stderr, "ERROR: Output file %s cannot be
opened!\n", ovalue);
```

**Improper Resource Access Authorization\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3630 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 347 | 347 |
| Object | fprintf | fprintf |

Code Snippet

| | |
|---|---|
| File Name | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Method | int main(int argc, char *argv[]) |

```
....
347.                  fprintf(stderr,"ERROR: Cannot create temp dir
%s!\n", DLT_CONVERT_WS);
```

**Improper Resource Access Authorization\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3631 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 358 | 358 |
| Object | fprintf | fprintf |

Code Snippet

| | |
|---|---|
| File Name | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Method | int main(int argc, char *argv[]) |

```
....
358.                    fprintf(stderr, "ERROR: %s is not a directory",
DLT_CONVERT_WS);
```

**Improper Resource Access Authorization\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3632 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 376 | 376 |
| Object | fprintf | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
376.                    fprintf(stderr, "ERROR: Failed to execute command
[%s] with error [%d]\n",
```

**Improper Resource Access Authorization\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3633 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 382 | 382 |
| Object | fprintf | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
382.                fprintf(stderr,"ERROR: Cannot scan temp dir %s!\n",
DLT_CONVERT_WS);
```

**Improper Resource Access Authorization\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3634 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 420 | 420 |
| Object | fprintf | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
420.                    fprintf(stderr, "ERROR: Selected first message %d
is out of range!\n", begin);
```

## 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=1000013&projectid=8&pathid=4050 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 950 | 950 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
950.        node->data[len] = 0;
```

**Unchecked Array Index\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4051 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 950 | 950 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
950.        node->data[len] = 0;
```

**Unchecked Array Index\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4052 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 950 | 950 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
950.        node->data[len] = 0;
```

**Unchecked Array Index\Path 4:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4053 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 959 | 959 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
959.        node->data[len] = 0;
```

**Unchecked Array Index\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4054 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 959 | 959 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
959.        node->data[len] = 0;
```

**Unchecked Array Index\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4055 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 959 | 959 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
959.        node->data[len] = 0;
```

**Unchecked Array Index\Path 7:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4056
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 977 | 977 |
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
977.        node->data[len] = 0;
```

**Unchecked Array Index\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4057
Status New

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Line | 995 | 995 |

| | | |
|---|---|---|
| Object | len | len |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c
Method static cmark_node *handle_pointy_brace(subject *subj, int options) {

```
....
995.      node->data[len] = 0;
```

**Unchecked Array Index\Path 9:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4058
Status New

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.12.1-CVE-2022-27650-TP.c | containers@@crun-0.12.1-CVE-2022-27650-TP.c |
| Line | 84 | 84 |
| Object | env_size | env_size |

Code Snippet
File Name containers@@crun-0.12.1-CVE-2022-27650-TP.c
Method append_env (const char *arg)

```
....
84.    exec_options.env[exec_options.env_size] = xstrdup (arg);
```

**Unchecked Array Index\Path 10:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4059
Status New

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.14.1-CVE-2022-27650-TP.c | containers@@crun-0.14.1-CVE-2022-27650-TP.c |
| Line | 84 | 84 |
| Object | env_size | env_size |

Code Snippet
File Name containers@@crun-0.14.1-CVE-2022-27650-TP.c
Method append_env (const char *arg)

```
....
84.    exec_options.env[exec_options.env_size] = xstrdup (arg);
```

**Unchecked Array Index\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4060 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.15.1-CVE-2022-27650-TP.c | containers@@crun-0.15.1-CVE-2022-27650-TP.c |
| Line | 85 | 85 |
| Object | env_size | env_size |

Code Snippet
File Name containers@@crun-0.15.1-CVE-2022-27650-TP.c
Method append_env (const char *arg)

```
....
85.    exec_options.env[exec_options.env_size] = xstrdup (arg);
```

**Unchecked Array Index\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4061 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.19.1-CVE-2022-27650-TP.c | containers@@crun-0.19.1-CVE-2022-27650-TP.c |
| Line | 85 | 85 |
| Object | env_size | env_size |

Code Snippet
File Name containers@@crun-0.19.1-CVE-2022-27650-TP.c
Method append_env (const char *arg)

```
....
85.    exec_options.env[exec_options.env_size] = xstrdup (arg);
```

**Unchecked Array Index\Path 13:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4062 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | containers@@crun-1.4.1-CVE-2022-27650-TP.c | containers@@crun-1.4.1-CVE-2022-27650-TP.c |
| Line | 97 | 97 |
| Object | env_size | env_size |

Code Snippet
File Name containers@@crun-1.4.1-CVE-2022-27650-TP.c
Method append_env (const char *arg)

```
....
97.    exec_options.env[exec_options.env_size] = xstrdup (arg);
```

**Unchecked Array Index\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4063 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8177-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8177-TP.c |
| Line | 261 | 261 |
| Object | len | len |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8177-TP.c
Method static char *parse_filename(const char *ptr, size_t len)

```
....
261.    copy[len] = '\0';
```

**Unchecked Array Index\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4064 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 865 | 865 |
| Object | s | s |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static int waitconnect_getsock(struct connectdata *conn,

```
....
865.        sock[s] = conn->tempsock[i];
```

**Unchecked Array Index\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4065
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 830 | 830 |
| Object | s | s |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static int ftp_domore_getsock(struct connectdata *conn, curl_socket_t *socks)

```
....
830.            socks[s] = conn->tempsock[i];
```

**Unchecked Array Index\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4066
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c |
| Line | 3199 | 3199 |

| | | |
|---|---|---|
| Object | pathLen | pathLen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_done(struct connectdata *conn, CURLcode status,

```
....
3199.          rawPath[pathLen] = '\0';
```

**Unchecked Array Index\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4067
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 1465 | 1465 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method gtls_connect_step3(struct connectdata *conn,

```
....
1465.    conn->recv[sockindex] = gtls_recv;
```

**Unchecked Array Index\Path 19:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4068
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 1466 | 1466 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method gtls_connect_step3(struct connectdata *conn,

```
....
1466.    conn->send[sockindex] = gtls_send;
```

**Unchecked Array Index\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4069 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 220 | 220 |
| Object | n | n |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method get_alg_id_by_name(char *name)

```
....
220.    tmp[n] = 0;
```

**Unchecked Array Index\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4070 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 1441 | 1441 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_connect_common(struct connectdata *conn, int sockindex,

```
....
1441.      conn->recv[sockindex] = schannel_recv;
```

**Unchecked Array Index\Path 22:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4071 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 1442 | 1442 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_connect_common(struct connectdata *conn, int sockindex,

```
....
1442.       conn->send[sockindex] = schannel_send;
```

**Unchecked Array Index\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4072 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 865 | 865 |
| Object | s | s |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static int waitconnect_getsock(struct connectdata *conn,

```
....
865.        sock[s] = conn->tempsock[i];
```

**Unchecked Array Index\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4073 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 715 | 715 |
| Object | certnum | certnum |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
715.    ci->certinfo[certnum] = nl;
```

**Unchecked Array Index\Path 25:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4074
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 789 | 789 |
| Object | stripped_pem_count | stripped_pem_count |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method static CURLcode pubkey_pem_to_der(const char *pem,

```
....
789.    stripped_pem[stripped_pem_count] = '\0';
```

**Unchecked Array Index\Path 26:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4075
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c |
| Line | 1379 | 1379 |

| | | |
|---|---|---|
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c
Method int Curl_single_getsock(const struct connectdata *conn,

```
....
1379.       sock[sockindex] = conn->sockfd;
```

**Unchecked Array Index\Path 27:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4076
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c |
| Line | 1394 | 1394 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c
Method int Curl_single_getsock(const struct connectdata *conn,

```
....
1394.         sock[sockindex] = conn->writesockfd;
```

**Unchecked Array Index\Path 28:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4077
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c |
| Line | 271 | 271 |
| Object | len | len |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c
Method char *Curl_copy_header_value(const char *header)

```
....
271.    value[len] = 0; /* zero terminate */
```

**Unchecked Array Index\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4078 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 759 | 759 |
| Object | pathlen | pathlen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
759.            co->path[pathlen] = 0; /* zero terminate */
```

**Unchecked Array Index\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4079 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1079 | 1079 |
| Object | myhash | myhash |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1079.        c->cookies[myhash] = co;
```

**Unchecked Array Index\Path 31:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4080 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 1559 | 1559 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static void Curl_nss_close(struct connectdata *conn, int sockindex)

```
....
1559.       conn->sock[sockindex] = CURL_SOCKET_BAD;
```

**Unchecked Array Index\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4081 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 2236 | 2236 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static CURLcode nss_connect_common(struct connectdata *conn, int sockindex,

```
....
2236.     conn->recv[sockindex] = nss_recv;
```

**Unchecked Array Index\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4082 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 2237 | 2237 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static CURLcode nss_connect_common(struct connectdata *conn, int sockindex,

```
....
2237.    conn->send[sockindex] = nss_send;
```

**Unchecked Array Index\Path 34:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4083
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 759 | 759 |
| Object | pathlen | pathlen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
759.            co->path[pathlen] = 0; /* zero terminate */
```

**Unchecked Array Index\Path 35:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4084
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1079 | 1079 |

| | | |
|---|---|---|
| Object | myhash | myhash |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1079.         c->cookies[myhash] = co;
```

**Unchecked Array Index\Path 36:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4085
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 759 | 759 |
| Object | pathlen | pathlen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
759.             co->path[pathlen] = 0; /* zero terminate */
```

**Unchecked Array Index\Path 37:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4086
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1079 | 1079 |
| Object | myhash | myhash |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method Curl_cookie_add(struct Curl_easy *data,

```
....
1079.         c->cookies[myhash] = co;
```

**Unchecked Array Index\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4087 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |
| Line | 893 | 893 |
| Object | s | s |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c
Method static int waitconnect_getsock(struct connectdata *conn,

```
....
893.         sock[s] = conn->tempsock[i];
```

**Unchecked Array Index\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4088 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c |
| Line | 834 | 834 |
| Object | s | s |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c
Method static int ftp_domore_getsock(struct connectdata *conn, curl_socket_t *socks)

```
....
834.             socks[s] = conn->tempsock[i];
```

**Unchecked Array Index\Path 40:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4089 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c |
| Line | 3215 | 3215 |
| Object | pathLen | pathLen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8285-TP.c
Method static CURLcode ftp_done(struct connectdata *conn, CURLcode status,

```
....
3215.          rawPath[pathLen] = '\0';
```

**Unchecked Array Index\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4090 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 4050 | 4050 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static CURLcode ossl_connect_common(struct connectdata *conn,

```
....
4050.      conn->recv[sockindex] = ossl_recv;
```

**Unchecked Array Index\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4091 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 4051 | 4051 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method static CURLcode ossl_connect_common(struct connectdata *conn,

```
....
4051.      conn->send[sockindex] = ossl_send;
```

**Unchecked Array Index\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4092
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 1264 | 1264 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c
Method gtls_connect_step3(struct connectdata *conn,

```
....
1264.    conn->recv[sockindex] = gtls_recv;
```

**Unchecked Array Index\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4093
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 1265 | 1265 |

| | | |
|---|---|---|
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c
Method gtls_connect_step3(struct connectdata *conn,

```
....
1265.    conn->send[sockindex] = gtls_send;
```

**Unchecked Array Index\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4094
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 211 | 211 |
| Object | n | n |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method get_alg_id_by_name(char *name)

```
....
211.    tmp[n] = 0;
```

**Unchecked Array Index\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4095
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 1569 | 1569 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_connect_common(struct connectdata *conn, int sockindex,

```
....
1569.       conn->recv[sockindex] = schannel_recv;
```

**Unchecked Array Index\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4096 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 1570 | 1570 |
| Object | sockindex | sockindex |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_connect_common(struct connectdata *conn, int sockindex,

```
....
1570.       conn->send[sockindex] = schannel_send;
```

**Unchecked Array Index\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4097 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Line | 893 | 893 |
| Object | s | s |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c
Method static int waitconnect_getsock(struct connectdata *conn,

```
....
893.        sock[s] = conn->tempsock[i];
```

**Unchecked Array Index\Path 49:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4098 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 744 | 744 |
| Object | certnum | certnum |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_push_certinfo_len(struct Curl_easy *data,

```
....
744.    ci->certinfo[certnum] = nl;
```

**Unchecked Array Index\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4099 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 818 | 818 |
| Object | stripped_pem_count | stripped_pem_count |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method static CURLcode pubkey_pem_to_der(const char *pem,

```
....
818.    stripped_pem[stripped_pem_count] = '\0';
```

## 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=1000013&projectid=8&pathid=1665 |
| Status | New |

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 221 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-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 | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 347 | 347 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
347.                    snprintf(time_buf, sizeof(time_buf), "%ld",
```

**Unchecked Return Value\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1666 |
| Status | New |

The qb_log_blackbox_open method calls the snprintf function, at line 144 of ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-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 | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 149 | 149 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_open(struct qb_log_target *t)

```
....
149.        snprintf(t->filename, PATH_MAX, "%s-%d-blackbox", t->name,
getpid());
```

**Unchecked Return Value\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1667 |
| Status | New |

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 221 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 347 | 347 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
347.                    snprintf(time_buf, sizeof(time_buf), "%ld",
```

**Unchecked Return Value\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1668 |
| Status | New |

The qb_log_blackbox_open method calls the snprintf function, at line 144 of ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 149 | 149 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_open(struct qb_log_target *t)

```
....
149.        snprintf(t->filename, PATH_MAX, "%s-%d-blackbox", t->name,
getpid());
```

**Unchecked Return Value\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1669 |
| Status | New |

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 221 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 347 | 347 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
347.                    snprintf(time_buf, sizeof(time_buf), "%ld",
```

**Unchecked Return Value\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1670 |
| Status | New |

The qb_log_blackbox_open method calls the snprintf function, at line 144 of ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 149 | 149 |
| Object | snprintf | snprintf |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Method | qb_log_blackbox_open(struct qb_log_target *t) |

```
....
149.        snprintf(t->filename, PATH_MAX, "%s-%d-blackbox", t->name,
getpid());
```

**Unchecked Return Value\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1671 |
| Status | New |

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 221 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 347 | 347 |
| Object | snprintf | snprintf |

Code Snippet

| | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
347.                    snprintf(time_buf, sizeof(time_buf), "%ld",
```

**Unchecked Return Value\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1672 |
| Status | New |

The qb_log_blackbox_open method calls the snprintf function, at line 144 of ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 149 | 149 |
| Object | snprintf | snprintf |

| Code Snippet | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Method | qb_log_blackbox_open(struct qb_log_target *t) |

```
....
149.        snprintf(t->filename, PATH_MAX, "%s-%d-blackbox", t->name,
getpid());
```

**Unchecked Return Value\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1673 |
| Status | New |

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 221 of ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c |
| Line | 347 | 347 |
| Object | snprintf | snprintf |

| Code Snippet | |
|---|---|
| File Name | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c |
| Method | qb_log_blackbox_print_from_file(const char *bb_filename) |

```
....
347.                    snprintf(time_buf, sizeof(time_buf), "%ld",
```

**Unchecked Return Value\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1674 |
| Status | New |

The qb_log_blackbox_open method calls the snprintf function, at line 144 of ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c |
| Line | 149 | 149 |

| | | |
|---|---|---|
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c
Method qb_log_blackbox_open(struct qb_log_target *t)

```
....
149.        snprintf(t->filename, PATH_MAX, "%s-%d-blackbox", t->name,
getpid());
```

**Unchecked Return Value\Path 11:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1675
Status New

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 220 of ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c |
| Line | 347 | 347 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
347.                    snprintf(time_buf+slen, sizeof(time_buf) - slen,
".%03llu", timestamp.tv_nsec/QB_TIME_NS_IN_MSEC);
```

**Unchecked Return Value\Path 12:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1676
Status New

The qb_log_blackbox_print_from_file method calls the snprintf function, at line 220 of ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.7-CVE-2023- | ClusterLabs@@libqb-v2.0.7-CVE-2023- |

| | | |
|---|---|---|
| | 39976-TP.c | 39976-TP.c |
| Line | 349 | 349 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
349.                    snprintf(time_buf, sizeof(time_buf), "%ld",
```

**Unchecked Return Value\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1677 |
| Status | New |

The qb_log_blackbox_open method calls the snprintf function, at line 143 of ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-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 | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c |
| Line | 148 | 148 |
| Object | snprintf | snprintf |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c
Method qb_log_blackbox_open(struct qb_log_target *t)

```
....
148.        snprintf(t->filename, PATH_MAX, "%s-%d-blackbox", t->name,
getpid());
```

**Unchecked Return Value\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1678 |
| Status | New |

The = method calls the calloc function, at line 87 of commonmark@@cmark-0.30.0-CVE-2023-22484-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 | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 87 | 87 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 15:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1679
Status New

The = method calls the calloc function, at line 99 of commonmark@@cmark-0.30.0-CVE-2023-22484-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 | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 99 | 99 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1680
Status New

The = method calls the calloc function, at line 87 of commonmark@@cmark-0.30.0-CVE-2023-22486-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 | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 87 | 87 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1681
Status New

The = method calls the calloc function, at line 99 of commonmark@@cmark-0.30.0-CVE-2023-22486-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 | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 99 | 99 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1682
Status New

The = method calls the calloc function, at line 87 of commonmark@@cmark-0.30.0-CVE-2023-28626-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 | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 87 | 87 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 19:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1683
Status New

The = method calls the calloc function, at line 99 of commonmark@@cmark-0.30.0-CVE-2023-28626-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 | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 99 | 99 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 20:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1684
Status New

The = method calls the calloc function, at line 87 of commonmark@@cmark-0.30.2-CVE-2023-22484-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 | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 87 | 87 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 21:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1685
Status New

The = method calls the calloc function, at line 99 of commonmark@@cmark-0.30.2-CVE-2023-22484-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 | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 99 | 99 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 22:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1686
Status New

The = method calls the calloc function, at line 87 of commonmark@@cmark-0.30.2-CVE-2023-22486-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 | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 87 | 87 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 23:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1687
Status New

The = method calls the calloc function, at line 99 of commonmark@@cmark-0.30.2-CVE-2023-22486-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 | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 99 | 99 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 24:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1688
Status New

The = method calls the calloc function, at line 87 of commonmark@@cmark-0.30.2-CVE-2023-28626-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 | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 87 | 87 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
87.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 25:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1689
Status New

The = method calls the calloc function, at line 99 of commonmark@@cmark-0.30.2-CVE-2023-28626-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 | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 99 | 99 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
99.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 26:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1690
Status New

The = method calls the calloc function, at line 89 of commonmark@@cmark-0.30.3-CVE-2023-28626-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 | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 89 | 89 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));

```
....
89.    cmark_node *e = (cmark_node *)subj->mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 27:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1691
Status New

The = method calls the calloc function, at line 101 of commonmark@@cmark-0.30.3-CVE-2023-28626-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 | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 101 | 101 |
| Object | calloc | calloc |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));

```
....
101.    cmark_node *e = (cmark_node *)mem->calloc(1, sizeof(*e));
```

**Unchecked Return Value\Path 28:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1692
Status New

The main method calls the snprintf function, at line 191 of COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 368 | 368 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
368.                    snprintf(command, COMMAND_SIZE, "tar xf %s -C %s",
```

**Unchecked Return Value\Path 29:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1693
Status New

The main method calls the snprintf function, at line 191 of COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 371 | 371 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
371.                    snprintf(command, COMMAND_SIZE, "cp %s %s",
```

**Unchecked Return Value\Path 30:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1694
Status New

The main method calls the snprintf function, at line 191 of COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 396 | 396 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
396.              snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

**Unchecked Return Value\Path 31:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1695
Status New

The empty_dir method calls the snprintf function, at line 140 of COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 164 | 164 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
164.                      snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

**Unchecked Return Value\Path 32:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1696
Status New

The main method calls the snprintf function, at line 191 of COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Line | 395 | 395 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
395.              snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

**Unchecked Return Value\Path 33:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1697
Status New

The empty_dir method calls the snprintf function, at line 140 of COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Line | 164 | 164 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
164.                      snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

**Unchecked Return Value\Path 34:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1698

| Status | New |
|---|---|

The main method calls the snprintf function, at line 191 of COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Line | 395 | 395 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
395.              snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

**Unchecked Return Value\Path 35:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1699 |
| Status | New |

The empty_dir method calls the snprintf function, at line 140 of COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Line | 164 | 164 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
164.                      snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

**Unchecked Return Value\Path 36:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1700 |
| Status | New |

The dlt_json_filter_save method calls the sprintf function, at line 889 of COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 905 | 905 |
| Object | sprintf | sprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
905.          sprintf(filter_name, "filter%i", num);
```

**Unchecked Return Value\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1701 |
| Status | New |

The dlt_json_filter_save method calls the snprintf function, at line 889 of COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 933 | 933 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
933.      snprintf(filter_buffer, filter_buffer_size,
json_encoder_buffer(j_encoder));
```

**Unchecked Return Value\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1702 |
| Status | New |

The dlt_json_filter_save method calls the sprintf function, at line 848 of COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 861 | 861 |
| Object | sprintf | sprintf |

Code Snippet

File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c

Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
861.          sprintf(filter_name, "filter%i", num);
```

**Unchecked Return Value\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1703 |
| Status | New |

The main method calls the snprintf function, at line 191 of COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c |
| Line | 395 | 395 |
| Object | snprintf | snprintf |

Code Snippet

File Name COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c

Method int main(int argc, char *argv[])

```
....
395.              snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
```

**Unchecked Return Value\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1704 |
| Status | New |

The empty_dir method calls the snprintf function, at line 140 of COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c |
| Line | 164 | 164 |
| Object | snprintf | snprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
164.                      snprintf(tmp_filename, FILENAME_SIZE, "%s%s",
dir, files[i]->d_name);
```

**Unchecked Return Value\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1705 |
| Status | New |

The dlt_json_filter_save method calls the sprintf function, at line 885 of COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 901 | 901 |
| Object | sprintf | sprintf |

Code Snippet

| | |
|---|---|
| File Name | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Method | DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose) |

```
....
901.          sprintf(filter_name, "filter%i", num);
```

**Unchecked Return Value\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1706 |
| Status | New |

The dlt_json_filter_save method calls the snprintf function, at line 885 of COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 929 | 929 |
| Object | snprintf | snprintf |

Code Snippet

| | |
|---|---|
| File Name | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Method | DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose) |

```
....
929.      snprintf(filter_buffer, filter_buffer_size,
json_encoder_buffer(j_encoder));
```

**Unchecked Return Value\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1707 |
| Status | New |

The dlt_json_filter_save method calls the sprintf function, at line 844 of COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 857 | 857 |

| | | |
|---|---|---|
| Object | sprintf | sprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
857.          sprintf(filter_name, "filter%i", num);
```

**Unchecked Return Value\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1708
Status New

The schannel_connect_step2 method calls the malloc function, at line 860 of curl@@curl-curl-7_69_0-CVE-2021-22897-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_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 963 | 963 |
| Object | malloc | malloc |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_connect_step2(struct connectdata *conn, int sockindex)

```
....
963.      InitSecBuffer(&inbuf[0], SECBUFFER_TOKEN, malloc(BACKEND-
>encdata_offset),
```

**Unchecked Return Value\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1709
Status New

The *Curl_add_buffer_init method calls the calloc function, at line 1134 of curl@@curl-curl-7_69_0-CVE-2022-27776-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_69_0-CVE-2022- | curl@@curl-curl-7_69_0-CVE-2022- |

| | | |
|---|---|---|
| | 27776-TP.c | 27776-TP.c |
| Line | 1136 | 1136 |
| Object | calloc | calloc |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27776-TP.c
Method Curl_send_buffer *Curl_add_buffer_init(void)

```
....
1136.    return calloc(1, sizeof(Curl_send_buffer));
```

**Unchecked Return Value\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1710 |
| Status | New |

The *nss_sslver_to_name method calls the strdup function, at line 258 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 262 | 262 |
| Object | strdup | strdup |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
262.      return strdup("SSLv2");
```

**Unchecked Return Value\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1711 |
| Status | New |

The *nss_sslver_to_name method calls the strdup function, at line 258 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 264 | 264 |
| Object | strdup | strdup |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
264.      return strdup("SSLv3");
```

**Unchecked Return Value\Path 48:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1712
Status New

The *nss_sslver_to_name method calls the strdup function, at line 258 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 266 | 266 |
| Object | strdup | strdup |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
266.      return strdup("TLSv1.0");
```

**Unchecked Return Value\Path 49:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1713
Status New

The *nss_sslver_to_name method calls the strdup function, at line 258 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 269 | 269 |
| Object | strdup | strdup |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
269.      return strdup("TLSv1.1");
```

**Unchecked Return Value\Path 50:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1714
Status New

The *nss_sslver_to_name method calls the strdup function, at line 258 of curl@@curl-curl-7_69_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_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 273 | 273 |
| Object | strdup | strdup |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static char *nss_sslver_to_name(PRUint16 nssver)

```
....
273.      return strdup("TLSv1.2");
```

## 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=1000013&projectid=8&pathid=2334 |
| Status | New |

The variable declared in null at cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c in line 115 is not initialized when it is used by refs at cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c in line 89.

| | Source | Destination |
|---|---|---|
| File | cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c | cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c |
| Line | 117 | 91 |
| Object | null | refs |

Code Snippet

File Name cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c

Method cockpit_http_client_ensure (const gchar *name)

```
....
117.    CockpitHttpClient *client = NULL;
```

File Name cockpit-project@@cockpit-newest-CVE-2021-3520-FP.c

Method cockpit_http_client_ref (CockpitHttpClient *client)

```
....
91.    client->refs++;
```

**NULL Pointer Dereference\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2335 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by list_type at commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c |
| Line | 948 | 510 |
| Object | null | list_type |

Code Snippet

File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c

Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c

Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
510.    return (list_data->list_type == item_data->list_type &&
```

**NULL Pointer Dereference\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2336 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by delimiter at commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c |
| Line | 948 | 511 |
| Object | null | delimiter |

Code Snippet

File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c

Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c

Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
511.            list_data->delimiter == item_data->delimiter &&
```

**NULL Pointer Dereference\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2337 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by bullet_char at commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c |
| Line | 948 | 513 |
| Object | null | bullet_char |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.0-CVE-2023-24824-TP.c

Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
513.            list_data->bullet_char == item_data->bullet_char);
```

**NULL Pointer Dereference\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2338 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by list_type at commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Line | 948 | 510 |
| Object | null | list_type |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

| | |
|---|---|
| File Name | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Method | static int lists_match(cmark_list *list_data, cmark_list *item_data) { |

```
....
510.    return (list_data->list_type == item_data->list_type &&
```

**NULL Pointer Dereference\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2339 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by delimiter at commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Line | 948 | 511 |
| Object | null | delimiter |

Code Snippet

| | |
|---|---|
| File Name | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Method | static void open_new_blocks(cmark_parser *parser, cmark_node **container, |

```
....
948.    cmark_list *data = NULL;
```

| | |
|---|---|
| File Name | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Method | static int lists_match(cmark_list *list_data, cmark_list *item_data) { |

```
....
511.            list_data->delimiter == item_data->delimiter &&
```

**NULL Pointer Dereference\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2340 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by bullet_char at commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c |
| Line | 948 | 513 |
| Object | null | bullet_char |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.2-CVE-2023-24824-TP.c
Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
513.            list_data->bullet_char == item_data->bullet_char);
```

**NULL Pointer Dereference\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2341
Status New

The variable declared in null at commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by list_type at commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c |
| Line | 948 | 510 |
| Object | null | list_type |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c
Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
510.    return (list_data->list_type == item_data->list_type &&
```

**NULL Pointer Dereference\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2342 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by delimiter at commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c | commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c |
| Line | 948 | 511 |
| Object | null | delimiter |

Code Snippet

File Name commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c

Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c

Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
511.            list_data->delimiter == item_data->delimiter &&
```

**NULL Pointer Dereference\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2343 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c in line 945 is not initialized when it is used by bullet_char at commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c in line 509.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE- | commonmark@@cmark-0.30.3-CVE- |

| | | |
|---|---|---|
| | 2023-24824-TP.c | 2023-24824-TP.c |
| Line | 948 | 513 |
| Object | null | bullet_char |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
948.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.30.3-CVE-2023-24824-TP.c
Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
513.            list_data->bullet_char == item_data->bullet_char);
```

**NULL Pointer Dereference\Path 11:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2344
Status New

The variable declared in null at commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c in line 973 is not initialized when it is used by list_type at commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c in line 512.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c |
| Line | 976 | 513 |
| Object | null | list_type |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
976.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c
Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
513.    return (list_data->list_type == item_data->list_type &&
```

**NULL Pointer Dereference\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2345 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c in line 973 is not initialized when it is used by delimiter at commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c in line 512.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c | commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c |
| Line | 976 | 514 |
| Object | null | delimiter |

Code Snippet

File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c

Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
976.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c

Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
514.            list_data->delimiter == item_data->delimiter &&
```

**NULL Pointer Dereference\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2346 |
| Status | New |

The variable declared in null at commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c in line 973 is not initialized when it is used by bullet_char at commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c in line 512.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE- | commonmark@@cmark-0.31.0-CVE- |

| | | |
|---|---|---|
| | 2023-24824-TP.c | 2023-24824-TP.c |
| Line | 976 | 516 |
| Object | null | bullet_char |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c
Method static void open_new_blocks(cmark_parser *parser, cmark_node **container,

```
....
976.    cmark_list *data = NULL;
```

File Name commonmark@@cmark-0.31.0-CVE-2023-24824-TP.c
Method static int lists_match(cmark_list *list_data, cmark_list *item_data) {

```
....
516.            list_data->bullet_char == item_data->bullet_char);
```

**NULL Pointer Dereference\Path 14:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2347
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 2696 is not initialized when it is used by time at curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c in line 2696.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 2703 | 2730 |
| Object | null | time |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode add_next_timeout(struct curltime now,

```
....
2703.    struct time_node *node = NULL;
....
2730.      memcpy(tv, &node->time, sizeof(*tv));
```

**NULL Pointer Dereference\Path 15:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2348 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 415 is not initialized when it is used by cred at curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c in line 415.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c |
| Line | 430 | 508 |
| Object | null | cred |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
430.    struct curl_schannel_cred *old_cred = NULL;
....
508.                        BACKEND->cred->refcount));
```

**NULL Pointer Dereference\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2349 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 2696 is not initialized when it is used by time at curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c in line 2696.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 2703 | 2730 |
| Object | null | time |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode add_next_timeout(struct curltime now,

```
....
2703.    struct time_node *node = NULL;
....
2730.      memcpy(tv, &node->time, sizeof(*tv));
```

**NULL Pointer Dereference\Path 17:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2350 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3293 |
| Object | null | hostname_resolve |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3293.    Curl_safefree(conn->hostname_resolve);
```

**NULL Pointer Dereference\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2351 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by passwd at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3259 |
| Object | null | passwd |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3259.      Curl_safefree(conn->passwd);
```

**NULL Pointer Dereference\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2352 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by user at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3258 |
| Object | null | user |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3258.      Curl_safefree(conn->user);
```

**NULL Pointer Dereference\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2353 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by host at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3287 |
| Object | null | host |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3287.    Curl_safefree(conn->host.rawalloc);
```

**NULL Pointer Dereference\Path 21:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2354
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by host at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3285 |
| Object | null | host |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3285.    Curl_free_idnconverted_hostname(&conn->host);
```

**NULL Pointer Dereference\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2355 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by encalloc at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1535.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 1539 |
| Object | null | encalloc |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1539.      idn2_free(host->encalloc); /* must be freed with idn2_free()
since this was
```

**NULL Pointer Dereference\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2356 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by encalloc at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 1535.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 1538 |
| Object | null | encalloc |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1538.    if(host->encalloc) {
```

**NULL Pointer Dereference\Path 24:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2357
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3288 |
| Object | null | conn_to_host |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3288.    Curl_safefree(conn->conn_to_host.rawalloc);
```

**NULL Pointer Dereference\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2358 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3286 |
| Object | null | conn_to_host |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3286.    Curl_free_idnconverted_hostname(&conn->conn_to_host);
```

**NULL Pointer Dereference\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2359 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by http_proxy at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |

| | | |
|---|---|---|
| Line | 3343 | 3271 |
| Object | null | http_proxy |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3271.      Curl_safefree(conn->http_proxy.passwd);
```

**NULL Pointer Dereference\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2360 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by http_proxy at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3269 |
| Object | null | http_proxy |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3269.      Curl_safefree(conn->http_proxy.user);
```

**NULL Pointer Dereference\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2361 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3272 |
| Object | null | socks_proxy |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3272.      Curl_safefree(conn->socks_proxy.passwd);
```

**NULL Pointer Dereference\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2362 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3270 |
| Object | null | socks_proxy |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3270.      Curl_safefree(conn->socks_proxy.user);
```

**NULL Pointer Dereference\Path 30:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2363
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by handler at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3920.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3929 |
| Object | null | handler |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method CURLcode Curl_init_do(struct Curl_easy *data, struct connectdata *conn)

```
....
3929.          !(conn->handler->flags & PROTOPT_WILDCARD))
```

**NULL Pointer Dereference\Path 31:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2364 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by bits at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3267 |
| Object | null | bits |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3267.    if(conn->bits.proxy_user_passwd) {
```

**NULL Pointer Dereference\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2365 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3337 is not initialized when it is used by bits at curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c | curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c |
| Line | 3343 | 3256 |
| Object | null | bits |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-22576-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3256.    if(conn->bits.user_passwd) {
```

**NULL Pointer Dereference\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2366 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c in line 1747 is not initialized when it is used by data at curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c in line 1747.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c |
| Line | 1752 | 1785 |
| Object | null | data |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27774-TP.c

Method CURLcode Curl_retry_request(struct connectdata *conn,

```
....
1752.    *url = NULL;
....
1785.      infof(conn->data, "Connection died, retrying a fresh
connect\n");
```

**NULL Pointer Dereference\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2367 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 482 is not initialized when it is used by num_connections at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 89.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c |
| Line | 493 | 98 |
| Object | null | num_connections |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c
Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
493.    struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c
Method static int bundle_remove_conn(struct connectbundle *cb_ptr,

```
....
98.         cb_ptr->num_connections--;
```

**NULL Pointer Dereference\Path 35:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2368
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 482 is not initialized when it is used by conn_list at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 89.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c |
| Line | 493 | 97 |
| Object | null | conn_list |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c
Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
493.    struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c
Method static int bundle_remove_conn(struct connectbundle *cb_ptr,

```
....
97.         Curl_llist_remove(&cb_ptr->conn_list, curr, NULL);
```

**NULL Pointer Dereference\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2369 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 482 is not initialized when it is used by conn_list at curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c in line 89.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c |
| Line | 493 | 94 |
| Object | null | conn_list |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c

Method Curl_conncache_extract_oldest(struct Curl_easy *data)

```
....
493.    struct connectbundle *bundle_candidate = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27775-TP.c

Method static int bundle_remove_conn(struct connectbundle *cb_ptr,

```
....
94.    curr = cb_ptr->conn_list.head;
```

**NULL Pointer Dereference\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2370 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c in line 687 is not initialized when it is used by filename at curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c in line 687.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |

| | | |
|---|---|---|
| Line | 752 | 1985 |
| Object | null | filename |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
752.        mlfile = NULL;
....
1985.                   mlfile->filename, per->this_url);
```

**NULL Pointer Dereference\Path 38:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2371
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by hostname_resolve at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3293 |
| Object | null | hostname_resolve |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3293.    Curl_safefree(conn->hostname_resolve);
```

**NULL Pointer Dereference\Path 39:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2372

| Status | New |
|---|---|

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by passwd at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3259 |
| Object | null | passwd |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3259.      Curl_safefree(conn->passwd);
```

**NULL Pointer Dereference\Path 40:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2373 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by user at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3258 |
| Object | null | user |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3258.       Curl_safefree(conn->user);
```

**NULL Pointer Dereference\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2374 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by host at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3287 |
| Object | null | host |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.     struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3287.     Curl_safefree(conn->host.rawalloc);
```

**NULL Pointer Dereference\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2375 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by host at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3285 |
| Object | null | host |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3285.    Curl_free_idnconverted_hostname(&conn->host);
```

**NULL Pointer Dereference\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2376
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by encalloc at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 1535.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 1539 |
| Object | null | encalloc |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1539.      idn2_free(host->encalloc); /* must be freed with idn2_free()
since this was
```

**NULL Pointer Dereference\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2377 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by encalloc at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 1535.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 1538 |
| Object | null | encalloc |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method void Curl_free_idnconverted_hostname(struct hostname *host)

```
....
1538.    if(host->encalloc) {
```

**NULL Pointer Dereference\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2378 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022- | curl@@curl-curl-7_69_0-CVE-2022- |

| | | |
|---|---|---|
| | 27782-TP.c | 27782-TP.c |
| Line | 3343 | 3288 |
| Object | null | conn_to_host |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3288.    Curl_safefree(conn->conn_to_host.rawalloc);
```

**NULL Pointer Dereference\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2379
Status New

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by conn_to_host at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3286 |
| Object | null | conn_to_host |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3286.    Curl_free_idnconverted_hostname(&conn->conn_to_host);
```

**NULL Pointer Dereference\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2380 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by http_proxy at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3271 |
| Object | null | http_proxy |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3271.      Curl_safefree(conn->http_proxy.passwd);
```

**NULL Pointer Dereference\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2381 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by http_proxy at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |

| | | |
|---|---|---|
| Line | 3343 | 3269 |
| Object | null | http_proxy |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3269.      Curl_safefree(conn->http_proxy.user);
```

**NULL Pointer Dereference\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2382 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3272 |
| Object | null | socks_proxy |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c
Method static void reuse_conn(struct connectdata *old_conn,

```
....
3272.      Curl_safefree(conn->socks_proxy.passwd);
```

**NULL Pointer Dereference\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2383 |
| Status | New |

The variable declared in null at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3337 is not initialized when it is used by socks_proxy at curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c in line 3237.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c |
| Line | 3343 | 3270 |
| Object | null | socks_proxy |

Code Snippet

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static CURLcode create_conn(struct Curl_easy *data,

```
....
3343.    struct connectdata *conn_temp = NULL;
```

File Name curl@@curl-curl-7_69_0-CVE-2022-27782-TP.c

Method static void reuse_conn(struct connectdata *old_conn,

```
....
3270.      Curl_safefree(conn->socks_proxy.user);
```

## 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=1000013&projectid=8&pathid=3951 |
| Status | New |

The dlt_parse_config_param method in COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.5-CVE- | COVESA@@dlt-daemon-v2.18.5-CVE- |

| | | |
|---|---|---|
| | 2023-26257-TP.c | 2023-26257-TP.c |
| Line | 164 | 164 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.      pFile = fopen(filename, "r");
```

**TOCTOU\Path 2:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3952
Status New

The dlt_parse_config_param method in COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c |
| Line | 164 | 164 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.      pFile = fopen(filename, "r");
```

**TOCTOU\Path 3:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3953
Status New

The dlt_json_filter_save method in COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 930 | 930 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
930.      FILE *handle = fopen(filename, "w");
```

**TOCTOU\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3954 |
| Status | New |

The dlt_parse_config_param method in COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 173 | 173 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
173.      pFile = fopen(filename, "r");
```

**TOCTOU\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3955 |
| Status | New |

The dlt_json_filter_load method in COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 680 | 680 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
680.      handle = fopen(filename, "r");
```

**TOCTOU\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3956 |
| Status | New |

The dlt_json_filter_save method in COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 926 | 926 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
926.      FILE *handle = fopen(filename, "w");
```

**TOCTOU\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3957 |
| Status | New |

The dlt_parse_config_param method in COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 183 | 183 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
183.      pFile = fopen(filename, "r");
```

**TOCTOU\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3958
Status New

The dlt_json_filter_load method in COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-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 | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 676 | 676 |
| Object | fopen | fopen |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
676.      handle = fopen(filename, "r");
```

**TOCTOU\Path 9:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3959

| Status | New |
|---|---|

The load_file method in curl@@curl-curl-7_69_0-CVE-2021-22890-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_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 253 | 253 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
253.    f = fopen(file, "rb");
```

**TOCTOU\Path 10:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3960 |
| Status | New |

The Curl_pin_peer_pubkey method in curl@@curl-curl-7_69_0-CVE-2021-22924-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_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 888 | 888 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
888.    fp = fopen(pinnedpubkey, "rb");
```

**TOCTOU\Path 11:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8& |

| | |
|---|---|
| | pathid=3961 |
| Status | New |

The vms_realfilesize method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 166 | 166 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
166.    file = fopen(name, "r"); /* VMS */
```

**TOCTOU\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3962 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 875 | 875 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
875.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**TOCTOU\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |

| | |
|---|---|
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3963 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 913 | 913 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
913.              FILE *newfile = fopen(config->etag_save_file, "wb");
```

**TOCTOU\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3964 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 941 | 941 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
941.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

**TOCTOU\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3965 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 1083 | 1083 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1083.               FILE *file = fopen(outfile, "ab",
```

**TOCTOU\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3966 |
| Status | New |

The *Curl_cookie_init method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1134 | 1134 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1134.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3967 |
| Status | New |

The cookie_output method in curl@@curl-curl-7_69_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_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1537 | 1537 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1537.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3968 |
| Status | New |

The *Curl_cookie_init method in curl@@curl-curl-7_69_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_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1134 | 1134 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1134.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3969 |
| Status | New |

The cookie_output method in curl@@curl-curl-7_69_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_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1537 | 1537 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1537.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3970 |
| Status | New |

The *Curl_cookie_init method in curl@@curl-curl-7_69_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_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1134 | 1134 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1134.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3971 |
| Status | New |

The cookie_output method in curl@@curl-curl-7_69_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_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1537 | 1537 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1537.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 22:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3972 |
| Status | New |

The load_file method in curl@@curl-curl-7_71_0-CVE-2021-22890-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_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 176 | 176 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c

| | |
|---|---|
| Method | static gnutls_datum_t load_file(const char *file) |

```
....
176.     f = fopen(file, "rb");
```

**TOCTOU\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3973 |
| Status | New |

The schannel_connect_step1 method in curl@@curl-curl-7_71_0-CVE-2021-22897-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_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 616 | 616 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Method | schannel_connect_step1(struct connectdata *conn, int sockindex) |

```
....
616.             fInCert = fopen(data->set.ssl.cert, "rb");
```

**TOCTOU\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3974 |
| Status | New |

The Curl_pin_peer_pubkey method in curl@@curl-curl-7_71_0-CVE-2021-22924-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_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 917 | 917 |
| Object | fopen | fopen |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Method | CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data, |

```
....
917.    fp = fopen(pinnedpubkey, "rb");
```

**TOCTOU\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3975 |
| Status | New |

The vms_realfilesize method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 168 | 168 |
| Object | fopen | fopen |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Method | static curl_off_t vms_realfilesize(const char *name, |

```
....
168.    file = fopen(name, "r"); /* VMS */
```

**TOCTOU\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3976 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 878 | 878 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
878.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**TOCTOU\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3977 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 915 | 915 |
| Object | fopen | fopen |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
915.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

**TOCTOU\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3978 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 957 | 957 |

| | | |
|---|---|---|
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
957.              FILE *newfile = fopen(config->etag_save_file, "wb");
```

**TOCTOU\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3979 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 1086 | 1086 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1086.              FILE *file = fopen(outfile, "ab",
```

**TOCTOU\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3980 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |

| | | |
|---|---|---|
| Line | 1563 | 1563 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1563.               FILE *fInCert = fopen(config->cert + 8, "rb");
```

**TOCTOU\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3981 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 1606 | 1606 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1606.               FILE *fInCert = fopen(config->key + 8, "rb");
```

**TOCTOU\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3982 |
| Status | New |

The *Curl_cookie_init method in curl@@curl-curl-7_71_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_71_0-CVE-2022- | curl@@curl-curl-7_71_0-CVE-2022- |

| | | |
|---|---|---|
| | 27779-TP.c | 27779-TP.c |
| Line | 1133 | 1133 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1133.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 33:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3983
Status New

The cookie_output method in curl@@curl-curl-7_71_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_71_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c |
| Line | 1536 | 1536 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 34:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3984
Status New

The *Curl_cookie_init method in curl@@curl-curl-7_71_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_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1133 | 1133 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1133.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 35:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3985
Status New

The cookie_output method in curl@@curl-curl-7_71_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_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1536 | 1536 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 36:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3986
Status New

The *Curl_cookie_init method in curl@@curl-curl-7_71_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_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1133 | 1133 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1133.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 37:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3987
Status New

The cookie_output method in curl@@curl-curl-7_71_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_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1536 | 1536 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 38:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3988
Status New

The load_file method in curl@@curl-curl-7_73_0-CVE-2021-22890-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_73_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c |
| Line | 176 | 176 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
176.    f = fopen(file, "rb");
```

**TOCTOU\Path 39:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3989
Status New

The schannel_connect_step1 method in curl@@curl-curl-7_73_0-CVE-2021-22897-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_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 619 | 619 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
619.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

**TOCTOU\Path 40:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3990
Status New

The Curl_pin_peer_pubkey method in curl@@curl-curl-7_73_0-CVE-2021-22924-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_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 963 | 963 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
963.    fp = fopen(pinnedpubkey, "rb");
```

**TOCTOU\Path 41:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3991
Status New

The vms_realfilesize method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 168 | 168 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static curl_off_t vms_realfilesize(const char *name,

```
....
168.    file = fopen(name, "r"); /* VMS */
```

**TOCTOU\Path 42:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3992
Status New

The single_transfer method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 882 | 882 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
882.               newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**TOCTOU\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3993 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 919 | 919 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
919.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

**TOCTOU\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3994 |
| Status | New |

The single_transfer method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 961 | 961 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
961.              FILE *newfile = fopen(config->etag_save_file, "wb");
```

**TOCTOU\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3995
Status New

The single_transfer method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1099 | 1099 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1099.              FILE *file = fopen(outfile, "ab",
```

**TOCTOU\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3996
Status New

The single_transfer method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1579 | 1579 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1579.               FILE *fInCert = fopen(config->cert + 8, "rb");
```

**TOCTOU\Path 47:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3997
Status New

The single_transfer method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1622 | 1622 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1622.               FILE *fInCert = fopen(config->key + 8, "rb");
```

**TOCTOU\Path 48:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3998

| Status | New |
|---|---|

The *Curl_cookie_init method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1133 | 1133 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1133.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

**TOCTOU\Path 49:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3999 |
| Status | New |

The cookie_output method in curl@@curl-curl-7_73_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_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1536 | 1536 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**TOCTOU\Path 50:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8& |

| | |
|---|---|
| | pathid=4000 |
| Status | New |

The *Curl_cookie_init method in curl@@curl-curl-7_73_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_73_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c |
| Line | 1133 | 1133 |
| Object | fopen | fopen |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c
Method struct CookieInfo *Curl_cookie_init(struct Curl_easy *data,

```
....
1133.       fp = file?fopen(file, FOPEN_READTEXT):NULL;
```

## 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=1000013&projectid=8&pathid=3861 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c |
| Line | 164 | 164 |
| Object | pFile | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.      pFile = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3862 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c |
| Line | 164 | 164 |
| Object | pFile | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
164.      pFile = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3863 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 173 | 173 |
| Object | pFile | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
173.      pFile = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 4:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3864 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 680 | 680 |
| Object | handle | handle |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
680.      handle = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3865 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 183 | 183 |
| Object | pFile | pFile |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method int dlt_parse_config_param(char *config_id, char **config_data)

```
....
183.      pFile = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3866 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 676 | 676 |
| Object | handle | handle |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_load(DltFilter *filter, const char *filename, int verbose)

```
....
676.      handle = fopen(filename, "r");
```

**Incorrect Permission Assignment For Critical Resources\Path 7:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3867
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c |
| Line | 253 | 253 |
| Object | f | f |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
253.     f = fopen(file, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3868
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 888 | 888 |

| | | |
|---|---|---|
| Object | fp | fp |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
888.    fp = fopen(pinnedpubkey, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 9:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3869
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 166 | 166 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_69_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 10:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3870
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 875 | 875 |
| Object | newfile | newfile |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
875.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**Incorrect Permission Assignment For Critical Resources\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3871 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1537 | 1537 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1537.      out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3872 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1537 | 1537 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1537.      out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3873 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1537 | 1537 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1537.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3874 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c |
| Line | 176 | 176 |
| Object | f | f |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
176.     f = fopen(file, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3875 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c |
| Line | 616 | 616 |
| Object | fInCert | fInCert |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
616.            fInCert = fopen(data->set.ssl.cert, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3876
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 917 | 917 |
| Object | fp | fp |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
917.    fp = fopen(pinnedpubkey, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3877
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 168 | 168 |

| | | |
|---|---|---|
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_71_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 18:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3878
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 878 | 878 |
| Object | newfile | newfile |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
878.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**Incorrect Permission Assignment For Critical Resources\Path 19:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3879
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c |
| Line | 1536 | 1536 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3880 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1536 | 1536 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3881 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1536 | 1536 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 22:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3882 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c |
| Line | 176 | 176 |
| Object | f | f |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22890-TP.c
Method static gnutls_datum_t load_file(const char *file)

```
....
176.    f = fopen(file, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 23:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3883 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c |
| Line | 619 | 619 |
| Object | fInCert | fInCert |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct connectdata *conn, int sockindex)

```
....
619.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3884 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 963 | 963 |
| Object | fp | fp |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
963.    fp = fopen(pinnedpubkey, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 25:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3885
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 168 | 168 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_73_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 26:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3886
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 882 | 882 |

| | | |
|---|---|---|
| Object | newfile | newfile |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
882.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**Incorrect Permission Assignment For Critical Resources\Path 27:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3887
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1536 | 1536 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.      out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 28:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3888
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c |
| Line | 1536 | 1536 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3889 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_73_0-CVE-2022-35252-TP.c |
| Line | 1536 | 1536 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1536.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3890 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c |
| Line | 108 | 108 |
| Object | fp | fp |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22890-TP.c
Method static CURLcode load_cafile(const char *path, br_x509_trust_anchor **anchors,

```
....
108.    fp = fopen(path, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 31:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3891 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c |
| Line | 621 | 621 |
| Object | fInCert | fInCert |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22897-TP.c
Method schannel_connect_step1(struct Curl_easy *data, struct connectdata *conn,

```
....
621.            fInCert = fopen(data->set.ssl.primary.clientcert, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3892 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c |
| Line | 969 | 969 |
| Object | fp | fp |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method CURLcode Curl_pin_peer_pubkey(struct Curl_easy *data,

```
....
969.    fp = fopen(pinnedpubkey, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3893 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 168 | 168 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_75_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 34:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3894
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c |
| Line | 886 | 886 |
| Object | newfile | newfile |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
886.              newfile = fopen(config->headerfile, per->prev ==
NULL?"wb":"ab");
```

**Incorrect Permission Assignment For Critical Resources\Path 35:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3895
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27779-TP.c |
| Line | 1545 | 1545 |

| | | |
|---|---|---|
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1545.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 36:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3896
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_75_0-CVE-2022-32205-TP.c |
| Line | 1545 | 1545 |
| Object | out | out |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1545.       out = fopen(tempstore, FOPEN_WRITETEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 37:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3897
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c |
| Line | 930 | 930 |
| Object | handle | handle |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
930.      FILE *handle = fopen(filename, "w");
```

**Incorrect Permission Assignment For Critical Resources\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3898 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c |
| Line | 926 | 926 |
| Object | handle | handle |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2023-26257-TP.c
Method DltReturnValue dlt_json_filter_save(DltFilter *filter, const char *filename, int verbose)

```
....
926.      FILE *handle = fopen(filename, "w");
```

**Incorrect Permission Assignment For Critical Resources\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3899 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 913 | 913 |
| Object | newfile | newfile |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
913.              FILE *newfile = fopen(config->etag_save_file, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 40:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3900 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 941 | 941 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
941.            FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 41:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3901 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c |
| Line | 1083 | 1083 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1083.               FILE *file = fopen(outfile, "ab",
```

**Incorrect Permission Assignment For Critical Resources\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3902 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 915 | 915 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
915.             FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3903
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 957 | 957 |
| Object | newfile | newfile |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
957.               FILE *newfile = fopen(config->etag_save_file, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 44:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3904
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |

| | | |
|---|---|---|
| Line | 1086 | 1086 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1086.               FILE *file = fopen(outfile, "ab",
```

**Incorrect Permission Assignment For Critical Resources\Path 45:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3905
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 1563 | 1563 |
| Object | fInCert | fInCert |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1563.               FILE *fInCert = fopen(config->cert + 8, "rb");
```

**Incorrect Permission Assignment For Critical Resources\Path 46:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3906
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c |
| Line | 1606 | 1606 |
| Object | fInCert | fInCert |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27778-TP.c

| | |
|---|---|
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
1606.               FILE *fInCert = fopen(config->key + 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=1000013&projectid=8&pathid=3907 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 919 | 919 |
| Object | file | file |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
919.             FILE *file = fopen(config->etag_compare_file,
FOPEN_READTEXT);
```

**Incorrect Permission Assignment For Critical Resources\Path 48:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3908 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 961 | 961 |
| Object | newfile | newfile |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Method | static CURLcode single_transfer(struct GlobalConfig *global, |

```
....
961.               FILE *newfile = fopen(config->etag_save_file, "wb");
```

**Incorrect Permission Assignment For Critical Resources\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3909 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1099 | 1099 |
| Object | file | file |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1099.               FILE *file = fopen(outfile, "ab",
```

**Incorrect Permission Assignment For Critical Resources\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3910 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c |
| Line | 1579 | 1579 |
| Object | fInCert | fInCert |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27778-TP.c
Method static CURLcode single_transfer(struct GlobalConfig *global,

```
....
1579.               FILE *fInCert = fopen(config->cert + 8, "rb");
```

## 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=1000013&projectid=8&pathid=1872 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.12.1-CVE-2022-27650-TP.c | containers@@crun-0.12.1-CVE-2022-27650-TP.c |
| Line | 104 | 104 |
| Object | sizeof | sizeof |

Code Snippet
File Name containers@@crun-0.12.1-CVE-2022-27650-TP.c
Method static char **dup_array (char **arr, size_t len)

```
....
104.    ret = xmalloc (sizeof (char *) * (len + 1));
```

**Use of Sizeof On a Pointer Type\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1873 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.14.1-CVE-2022-27650-TP.c | containers@@crun-0.14.1-CVE-2022-27650-TP.c |
| Line | 104 | 104 |
| Object | sizeof | sizeof |

Code Snippet
File Name containers@@crun-0.14.1-CVE-2022-27650-TP.c
Method static char **dup_array (char **arr, size_t len)

```
....
104.    ret = malloc (sizeof (char *) * (len + 1));
```

**Use of Sizeof On a Pointer Type\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1874 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | containers@@crun-0.15.1-CVE-2022-27650-TP.c | containers@@crun-0.15.1-CVE-2022-27650-TP.c |
| Line | 106 | 106 |
| Object | sizeof | sizeof |

Code Snippet
File Name containers@@crun-0.15.1-CVE-2022-27650-TP.c
Method dup_array (char **arr, size_t len)

```
....
106.    ret = malloc (sizeof (char *) * (len + 1));
```

**Use of Sizeof On a Pointer Type\Path 4:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1875
Status New

| | Source | Destination |
|---|---|---|
| File | containers@@crun-0.19.1-CVE-2022-27650-TP.c | containers@@crun-0.19.1-CVE-2022-27650-TP.c |
| Line | 106 | 106 |
| Object | sizeof | sizeof |

Code Snippet
File Name containers@@crun-0.19.1-CVE-2022-27650-TP.c
Method dup_array (char **arr, size_t len)

```
....
106.    ret = malloc (sizeof (char *) * (len + 1));
```

**Use of Sizeof On a Pointer Type\Path 5:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1876
Status New

| | Source | Destination |
|---|---|---|
| File | containers@@crun-1.4.1-CVE-2022-27650-TP.c | containers@@crun-1.4.1-CVE-2022-27650-TP.c |
| Line | 118 | 118 |
| Object | sizeof | sizeof |

Code Snippet
File Name containers@@crun-1.4.1-CVE-2022-27650-TP.c
Method dup_array (char **arr, size_t len)

```
....
118.    ret = malloc (sizeof (char *) * (len + 1));
```

**Use of Sizeof On a Pointer Type\Path 6:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1877
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 2574 | 2574 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2574.                           sizeof(struct Curl_easy *), data))
```

**Use of Sizeof On a Pointer Type\Path 7:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1878
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c |
| Line | 2632 | 2632 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2020-8231-TP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2632.                               sizeof(struct Curl_easy *))) {
```

**Use of Sizeof On a Pointer Type\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1879 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 2574 | 2574 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2574.                           sizeof(struct Curl_easy *), data))
```

**Use of Sizeof On a Pointer Type\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1880 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c |
| Line | 2632 | 2632 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2632.                               sizeof(struct Curl_easy *))) {
```

**Use of Sizeof On a Pointer Type\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1881 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 669 | 669 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
669.    table = calloc((size_t) num, sizeof(struct curl_slist *));
```

**Use of Sizeof On a Pointer Type\Path 11:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1882 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1338 | 1338 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1338.       array = malloc(sizeof(struct Cookie *) * matches);
```

**Use of Sizeof On a Pointer Type\Path 12:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1883 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |

| | | |
|---|---|---|
| Line | 1348 | 1348 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1348.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

**Use of Sizeof On a Pointer Type\Path 13:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1884
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1552 | 1552 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1552.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

**Use of Sizeof On a Pointer Type\Path 14:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1885
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c |
| Line | 1566 | 1566 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27779-TP.c

| | |
|---|---|
| Method | static int cookie_output(struct Curl_easy *data, |

```
....
1566.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

**Use of Sizeof On a Pointer Type\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1886 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1338 | 1338 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1338.      array = malloc(sizeof(struct Cookie *) * matches);
```

**Use of Sizeof On a Pointer Type\Path 16:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1887 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1348 | 1348 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1348.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

**Use of Sizeof On a Pointer Type\Path 17:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1888 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1552 | 1552 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1552.      array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

**Use of Sizeof On a Pointer Type\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1889 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c |
| Line | 1566 | 1566 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1566.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

**Use of Sizeof On a Pointer Type\Path 19:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1890 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1338 | 1338 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1338.       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=1000013&projectid=8&pathid=1891 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1348 | 1348 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1348.       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=1000013&projectid=8&pathid=1892 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |

| | | |
|---|---|---|
| Line | 1552 | 1552 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1552.       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=1000013&projectid=8&pathid=1893
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c |
| Line | 1566 | 1566 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1566.       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=1000013&projectid=8&pathid=1894
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |
| Line | 2737 | 2737 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c

| | |
|---|---|
| Method | static CURLMcode singlesocket(struct Curl_multi *multi, |

```
....
2737.                                sizeof(struct Curl_easy *), data))
```

**Use of Sizeof On a Pointer Type\Path 24:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1895 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |
| Line | 2795 | 2795 |
| Object | sizeof | sizeof |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_71_0-CVE-2020-8231-TP.c |
| Method | static CURLMcode singlesocket(struct Curl_multi *multi, |

```
....
2795.                                sizeof(struct Curl_easy *))) {
```

**Use of Sizeof On a Pointer Type\Path 25:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1896 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Line | 2737 | 2737 |
| Object | sizeof | sizeof |

Code Snippet

| | |
|---|---|
| File Name | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Method | static CURLMcode singlesocket(struct Curl_multi *multi, |

```
....
2737.                                sizeof(struct Curl_easy *), data))
```

**Use of Sizeof On a Pointer Type\Path 26:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1897 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c |
| Line | 2795 | 2795 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2795.                                   sizeof(struct Curl_easy *))) {
```

**Use of Sizeof On a Pointer Type\Path 27:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1898 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 698 | 698 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
698.    table = calloc((size_t) num, sizeof(struct curl_slist *));
```

**Use of Sizeof On a Pointer Type\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1899 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c |
| Line | 1337 | 1337 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1337.       array = malloc(sizeof(struct Cookie *) * matches);
```

**Use of Sizeof On a Pointer Type\Path 29:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1900
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c |
| Line | 1347 | 1347 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1347.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

**Use of Sizeof On a Pointer Type\Path 30:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1901
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c |
| Line | 1551 | 1551 |

| | | |
|---|---|---|
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1551.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

**Use of Sizeof On a Pointer Type\Path 31:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1902
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c |
| Line | 1565 | 1565 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1565.       qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

**Use of Sizeof On a Pointer Type\Path 32:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1903
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1337 | 1337 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1337.       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=1000013&projectid=8&pathid=1904 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1347 | 1347 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1347.       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=1000013&projectid=8&pathid=1905 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1551 | 1551 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1551.       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=1000013&projectid=8&pathid=1906 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c |
| Line | 1565 | 1565 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1565.      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=1000013&projectid=8&pathid=1907 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1337 | 1337 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1337.      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=1000013&projectid=8&pathid=1908 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1347 | 1347 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1347.       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=1000013&projectid=8&pathid=1909
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1551 | 1551 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1551.       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=1000013&projectid=8&pathid=1910
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c | curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c |
| Line | 1565 | 1565 |

| | | |
|---|---|---|
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-35252-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1565.      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=1000013&projectid=8&pathid=1911
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c |
| Line | 2780 | 2780 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2780.                           sizeof(struct Curl_easy *), data))
```

**Use of Sizeof On a Pointer Type\Path 41:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1912
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c | curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c |
| Line | 2838 | 2838 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22901-FP.c
Method static CURLMcode singlesocket(struct Curl_multi *multi,

```
....
2838.                                   sizeof(struct Curl_easy *))) {
```

**Use of Sizeof On a Pointer Type\Path 42:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1913 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 744 | 744 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_init_certinfo(struct Curl_easy *data, int num)

```
....
744.    table = calloc((size_t) num, sizeof(struct curl_slist *));
```

**Use of Sizeof On a Pointer Type\Path 43:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1914 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1337 | 1337 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1337.      array = malloc(sizeof(struct Cookie *) * matches);
```

**Use of Sizeof On a Pointer Type\Path 44:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1915 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1347 | 1347 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1347.      qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

**Use of Sizeof On a Pointer Type\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1916 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1551 | 1551 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1551.      array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

**Use of Sizeof On a Pointer Type\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1917 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c |
| Line | 1565 | 1565 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27779-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1565.       qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

**Use of Sizeof On a Pointer Type\Path 47:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1918
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c |
| Line | 1337 | 1337 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1337.       array = malloc(sizeof(struct Cookie *) * matches);
```

**Use of Sizeof On a Pointer Type\Path 48:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1919
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c |
| Line | 1347 | 1347 |

| | | |
|---|---|---|
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c
Method struct Cookie *Curl_cookie_getlist(struct CookieInfo *c,

```
....
1347.       qsort(array, matches, sizeof(struct Cookie *), cookie_sort);
```

**Use of Sizeof On a Pointer Type\Path 49:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1920
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c |
| Line | 1551 | 1551 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1551.       array = calloc(1, sizeof(struct Cookie *) * c->numcookies);
```

**Use of Sizeof On a Pointer Type\Path 50:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1921
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c |
| Line | 1565 | 1565 |
| Object | sizeof | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32205-TP.c
Method static int cookie_output(struct Curl_easy *data,

```
....
1565.      qsort(array, nvalid, sizeof(struct Cookie *),
cookie_sort_ct);
```

## 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=1000013&projectid=8&pathid=2535 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 307 | 307 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
307.    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=1000013&projectid=8&pathid=2536 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 307 | 307 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
307.    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=1000013&projectid=8&pathid=2537 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 343 | 343 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
343.    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=1000013&projectid=8&pathid=2538 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 307 | 343 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
307.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
343.    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=1000013&projectid=8&pathid=2539 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 324 | 343 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
324.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
343.    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=1000013&projectid=8&pathid=2540 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 343 | 343 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
343.    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=1000013&projectid=8& |

| | |
|---|---|
| | pathid=2541 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 307 | 343 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
307.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
343.    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=1000013&projectid=8&pathid=2542 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 324 | 343 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
324.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
343.    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=1000013&projectid=8&pathid=2543 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 305 | 305 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    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=1000013&projectid=8&pathid=2544
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 305 | 305 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    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=1000013&projectid=8&pathid=2545
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 341 | 341 |

| | | |
|---|---|---|
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
341.    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=1000013&projectid=8&pathid=2546
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 305 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2547
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 322 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c

Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2548 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 341 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
341.    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=1000013&projectid=8&pathid=2549 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 305 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2550 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 322 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2551 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 305 | 305 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 18:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2552 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 305 | 305 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    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=1000013&projectid=8&pathid=2553 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 341 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
341.    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=1000013&projectid=8&pathid=2554 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 305 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2555 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 322 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2556 |

| Status | New |
|---|---|

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 341 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 23:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2557 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 305 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2558 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022- | curl@@curl-curl-7_73_0-CVE-2022- |

| | | |
|---|---|---|
| | 27781-TP.c | 27781-TP.c |
| Line | 322 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
341.    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=1000013&projectid=8&pathid=2559
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 305 | 305 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    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=1000013&projectid=8&pathid=2560
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 305 | 305 |
| Object | cipherlist | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Method | static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model, |

```
....
305.    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=1000013&projectid=8&pathid=2561 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 341 | 341 |
| Object | cipherlist | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Method | static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model, |

```
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 28:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2562 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 305 | 341 |
| Object | cipherlist | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Method | static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model, |

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 29:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2563 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 322 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 30:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2564 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 341 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 31:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2565 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 305 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 32:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2566 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 322 | 341 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
....
341.    for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 33:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2567 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 1241 | 1241 |
| Object | backends | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method static size_t Curl_multissl_version(char *buffer, size_t size)

```
....
1241.      char *end = backends + sizeof(backends);
```

**Sizeof Pointer Argument\Path 34:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2568 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 324 | 324 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
324.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 35:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2569 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 307 | 324 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
307.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
324.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 36:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2570 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 324 | 324 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
324.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 37:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8& |

| | |
|---|---|
| | pathid=2571 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 307 | 324 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
307.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
324.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 38:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2572 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 1270 | 1270 |
| Object | backends | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method static size_t Curl_multissl_version(char *buffer, size_t size)

```
....
1270.      char *end = backends + sizeof(backends);
```

**Sizeof Pointer Argument\Path 39:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2573 |
| Status | New |

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 322 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 40:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2574
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 305 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 41:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2575
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 322 | 322 |

| | | |
|---|---|---|
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 42:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2576
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 305 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 43:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2577
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 1316 | 1316 |
| Object | backends | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c

| | |
|---|---|
| Method | static size_t Curl_multissl_version(char *buffer, size_t size) |

```
....
1316.       char *end = backends + sizeof(backends);
```

**Sizeof Pointer Argument\Path 44:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2578 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 322 | 322 |
| Object | cipherlist | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Method | static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model, |

```
....
322.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 45:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2579 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 305 | 322 |
| Object | cipherlist | sizeof |

| | |
|---|---|
| Code Snippet | |
| File Name | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Method | static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model, |

```
....
305.     for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
322.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 46:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2580 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 322 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 47:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2581 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 305 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 48:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2582 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c |
| Line | 1287 | 1287 |
| Object | backends | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method static size_t multissl_version(char *buffer, size_t size)

```
....
1287.       char *end = backends + sizeof(backends);
```

**Sizeof Pointer Argument\Path 49:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2583 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 322 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
322.       for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

**Sizeof Pointer Argument\Path 50:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=2584 |
| Status | New |

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

| | | |
|---|---|---|
| | 27781-TP.c | 27781-TP.c |
| Line | 305 | 322 |
| Object | cipherlist | sizeof |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method static SECStatus set_ciphers(struct Curl_easy *data, PRFileDesc * model,

```
....
305.    for(i = 0; i < NUM_OF_CIPHERS; i++) {
....
322.      for(i = 0; i<NUM_OF_CIPHERS; i++) {
```

## 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=1000013&projectid=8&pathid=3930 |
| Status | New |

The system data read by qb_log_blackbox_print_from_file in the file ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c at line 221 is potentially exposed by qb_log_blackbox_print_from_file found in ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c at line 221.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c |
| Line | 290 | 290 |
| Object | perror | perror |

Code Snippet
File Name ClusterLabs@@libqb-v1.9.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
290.                    perror("ERROR: qb_rb_chunk_read failed");
```

**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=1000013&projectid=8&pathid=3931 |
| Status | New |

The system data read by qb_log_blackbox_print_from_file in the file ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c at line 221 is potentially exposed by qb_log_blackbox_print_from_file found in ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c at line 221.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c |
| Line | 290 | 290 |
| Object | perror | perror |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.1-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
290.                    perror("ERROR: qb_rb_chunk_read failed");
```

**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=1000013&projectid=8&pathid=3932 |
| Status | New |

The system data read by qb_log_blackbox_print_from_file in the file ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c at line 221 is potentially exposed by qb_log_blackbox_print_from_file found in ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c at line 221.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c |
| Line | 290 | 290 |
| Object | perror | perror |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.2-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
290.                    perror("ERROR: qb_rb_chunk_read failed");
```

**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=1000013&projectid=8&pathid=3933 |
| Status | New |

The system data read by qb_log_blackbox_print_from_file in the file ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c at line 221 is potentially exposed by qb_log_blackbox_print_from_file found in ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c at line 221.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c | ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c |
| Line | 290 | 290 |
| Object | perror | perror |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.4-CVE-2023-39976-FP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
290.                    perror("ERROR: qb_rb_chunk_read failed");
```

**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=1000013&projectid=8&pathid=3934 |
| Status | New |

The system data read by qb_log_blackbox_print_from_file in the file ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c at line 221 is potentially exposed by qb_log_blackbox_print_from_file found in ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c at line 221.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c |
| Line | 290 | 290 |
| Object | perror | perror |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.5-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
290.                    perror("ERROR: qb_rb_chunk_read failed");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 6:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3935 |
| Status | New |

The system data read by qb_log_blackbox_print_from_file in the file ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c at line 220 is potentially exposed by qb_log_blackbox_print_from_file found in ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c at line 220.

| | Source | Destination |
|---|---|---|
| File | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c | ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c |
| Line | 292 | 292 |
| Object | perror | perror |

Code Snippet
File Name ClusterLabs@@libqb-v2.0.7-CVE-2023-39976-TP.c
Method qb_log_blackbox_print_from_file(const char *bb_filename)

```
....
292.                    perror("ERROR: qb_rb_chunk_read failed");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 7:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3936 |
| Status | New |

The system data read by krb5_auth in the file curl@@curl-curl-7_69_0-CVE-2022-32208-TP.c at line 146 is potentially exposed by krb5_auth found in curl@@curl-curl-7_69_0-CVE-2022-32208-TP.c at line 146.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-32208-TP.c | curl@@curl-curl-7_69_0-CVE-2022-32208-TP.c |
| Line | 171 | 171 |
| Object | perror | perror |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-32208-TP.c
Method krb5_auth(void *app_data, struct connectdata *conn)

```
....
171.      perror("getsockname()");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3937 |
| Status | New |

The system data read by krb5_auth in the file curl@@curl-curl-7_71_0-CVE-2022-32208-TP.c at line 146 is potentially exposed by krb5_auth found in curl@@curl-curl-7_71_0-CVE-2022-32208-TP.c at line 146.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-32208-TP.c | curl@@curl-curl-7_71_0-CVE-2022-32208-TP.c |
| Line | 171 | 171 |
| Object | perror | perror |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-32208-TP.c
Method krb5_auth(void *app_data, struct connectdata *conn)

```
....
171.      perror("getsockname()");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 9:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3938 |
| Status | New |

The system data read by krb5_auth in the file curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c at line 206 is potentially exposed by krb5_auth found in curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c at line 206.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c | curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c |
| Line | 231 | 231 |
| Object | perror | perror |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-32208-TP.c
Method krb5_auth(void *app_data, struct connectdata *conn)

```
....
231.      perror("getsockname()");
```

**Exposure of System Data to Unauthorized Control Sphere\Path 10:**

| | |
|---|---|
| Severity | Low |

| | |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3939 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 158 | 157 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
158.                            dir, strerror(errno));
....
157.                    fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 11:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3940 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 168 | 167 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
168.                                    tmp_filename, strerror(errno));
....
167.                              fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 12:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3941 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 185 | 185 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.          fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 13:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3942 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Line | 158 | 157 |
| Object | errno | fprintf |

| | |
|---|---|
| Code Snippet | |
| File Name | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Method | void empty_dir(const char *dir) |

```
....
158.                            dir, strerror(errno));
....
157.                    fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 14:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3943 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Line | 168 | 167 |
| Object | errno | fprintf |

| | |
|---|---|
| Code Snippet | |
| File Name | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Method | void empty_dir(const char *dir) |

```
....
168.                                tmp_filename, strerror(errno));
....
167.                            fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 15:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3944 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|

| | | |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Line | 185 | 185 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.          fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 16:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3945
Status New

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Line | 158 | 157 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
158.                          dir, strerror(errno));
....
157.                  fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 17:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3946
Status New

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Line | 168 | 167 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
168.                                    tmp_filename, strerror(errno));
....
167.                            fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 18:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3947
Status New

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Line | 185 | 185 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.          fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, strerror(errno));
```

**Exposure of System Data to Unauthorized Control Sphere\Path 19:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3948 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c |
| Line | 158 | 157 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
158.                            dir, strerror(errno));
....
157.                    fprintf(stderr, "ERROR: Failed to scan %s with
error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 20:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3949 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c |
| Line | 168 | 167 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
168.                                    tmp_filename, strerror(errno));
....
167.                              fprintf(stderr, "ERROR: Failed to delete
%s with error %s\n",
```

**Exposure of System Data to Unauthorized Control Sphere\Path 21:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=3950 |
| Status | New |

The system data read by empty_dir in the file COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140 is potentially exposed by empty_dir found in COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c at line 140.

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c |
| Line | 185 | 185 |
| Object | errno | fprintf |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method void empty_dir(const char *dir)

```
....
185.          fprintf(stderr, "ERROR: Failed to stat %s with error
%s\n", dir, strerror(errno));
```

## 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=1000013&projectid=8&pathid=1937 |
| Status | New |

The buffer allocated by <= in commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c at line 193 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c |
| Line | 206 | 206 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22484-TP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
206.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 2:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1938
Status New

The buffer allocated by <= in commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c at line 193 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c |
| Line | 206 | 206 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-22486-TP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
206.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 3:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1939
Status New

The buffer allocated by <= in commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c at line 193 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c |
| Line | 206 | 206 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.0-CVE-2023-28626-FP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
206.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 4:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1940
Status New

The buffer allocated by <= in commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c at line 193 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c |
| Line | 206 | 206 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22484-TP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
206.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 5:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1941

| Status | New |
|---|---|

The buffer allocated by <= in commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c at line 193 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c | commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c |
| Line | 206 | 206 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-22486-TP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
206.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 6:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1942 |
| Status | New |

The buffer allocated by <= in commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c at line 193 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c |
| Line | 206 | 206 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.2-CVE-2023-28626-FP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
206.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 7:**

| Severity | Low |
|---|---|
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8& |

| | |
|---|---|
| | pathid=1943 |
| Status | New |

The buffer allocated by <= in commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c at line 195 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c | commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c |
| Line | 208 | 208 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.30.3-CVE-2023-28626-FP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
208.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 8:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1944 |
| Status | New |

The buffer allocated by <= in commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c at line 195 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c | commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c |
| Line | 208 | 208 |
| Object | <= | <= |

Code Snippet
File Name commonmark@@cmark-0.31.0-CVE-2023-28626-FP.c
Method static void subject_from_buf(cmark_mem *mem, int line_number, int block_offset, subject *e,

```
....
208.    for (i = 0; i <= MAXBACKTICKS; i++) {
```

**Potential Off by One Error in Loops\Path 9:**

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

| | |
|---|---|
| | PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1945 |
| Status | New |

The buffer allocated by <= in curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c at line 2142 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c |
| Line | 2147 | 2147 |
| Object | <= | <= |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2020-8286-TP.c
Method select_next_protocol(unsigned char **out, unsigned char *outlen,

```
....
2147.    for(i = 0; i + keylen <= inlen; i += in[i] + 1) {
```

**Potential Off by One Error in Loops\Path 10:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1946 |
| Status | New |

The buffer allocated by <= in curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c at line 2148 does not correctly account for the actual size of the value, resulting in an incorrect allocation that is off by one.

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c | curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c |
| Line | 2153 | 2153 |
| Object | <= | <= |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2020-8286-TP.c
Method select_next_protocol(unsigned char **out, unsigned char *outlen,

```
....
2153.    for(i = 0; i + keylen <= inlen; i += in[i] + 1) {
```

## 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=1000013&projectid=8&pathid=4042 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2021-22926-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22926-TP.c |
| Line | 853 | 853 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22926-TP.c
Method /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */

```
....
853.      /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */
```

**Information Exposure Through Comments\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4043 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c |
| Line | 357 | 357 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2022-27781-TP.c
Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....
357.   * 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=1000013&projectid=8&pathid=4044 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2021-22926-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22926-TP.c |
| Line | 853 | 853 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22926-TP.c
Method /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */

```
....
853.      /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */
```

**Information Exposure Through Comments\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4045 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c |
| Line | 355 | 355 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2022-27781-TP.c
Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....
355.   * Return true if at least one cipher-suite is enabled. Used to
determine
```

**Information Exposure Through Comments\Path 5:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4046 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2021-22926-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22926-TP.c |
| Line | 853 | 853 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22926-TP.c
Method /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */

```
....
853.      /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */
```

**Information Exposure Through Comments\Path 6:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4047
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c |
| Line | 355 | 355 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2022-27781-TP.c
Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....
355.   * Return true if at least one cipher-suite is enabled. Used to
determine
```

**Information Exposure Through Comments\Path 7:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4048
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2021-22926-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22926-TP.c |
| Line | 853 | 853 |

| | | |
|---|---|---|
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22926-TP.c
Method /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */

```
....
853.      /* New ChaCha20+Poly1305 cipher-suites used by TLS 1.3: */
```

**Information Exposure Through Comments\Path 8:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=4049
Status New

| | Source | Destination |
|---|---|---|
| File | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c | curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c |
| Line | 355 | 355 |
| Object | cipher- | cipher- |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2022-27781-TP.c
Method * Return true if at least one cipher-suite is enabled. Used to determine

```
....
355.   * Return true if at least one cipher-suite is enabled. Used to
determine
```

## Inconsistent Implementations

Query Path:
CPP\Cx\CPP Low Visibility\Inconsistent Implementations Version:0

*Description*

**Inconsistent Implementations\Path 1:**

Severity Low
Result State To Verify
Online Results http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1657
Status New

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Line | 232 | 232 |
| Object | getopt | getopt |

| | |
|---|---|
| Code Snippet | |
| File Name | COVESA@@dlt-daemon-v2.18.5-CVE-2022-39836-TP.c |
| Method | int main(int argc, char *argv[]) |

```
....
232.      while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

**Inconsistent Implementations\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1658 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Line | 231 | 231 |
| Object | getopt | getopt |

| | |
|---|---|
| Code Snippet | |
| File Name | COVESA@@dlt-daemon-v2.18.6-CVE-2022-39836-TP.c |
| Method | int main(int argc, char *argv[]) |

```
....
231.      while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

**Inconsistent Implementations\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1659 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Line | 231 | 231 |
| Object | getopt | getopt |

| | |
|---|---|
| Code Snippet | |
| File Name | COVESA@@dlt-daemon-v2.18.7-CVE-2022-39836-TP.c |
| Method | int main(int argc, char *argv[]) |

```
....
231.      while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

**Inconsistent Implementations\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1660 |
| Status | New |

| | Source | Destination |
|---|---|---|
| File | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c | COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c |
| Line | 231 | 231 |
| Object | getopt | getopt |

Code Snippet
File Name COVESA@@dlt-daemon-v2.18.8-CVE-2022-39836-TP.c
Method int main(int argc, char *argv[])

```
....
231.      while ((c = getopt (argc, argv, "vcashxmwtf:b:e:o:")) != -1) {
```

## 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=1000013&projectid=8&pathid=1661 |
| Status | New |

Method Curl_ssl_random at line 733 of curl@@curl-curl-7_69_0-CVE-2021-22924-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_69_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c |
| Line | 737 | 737 |

| | | |
|---|---|---|
| Object | random | random |

Code Snippet
File Name curl@@curl-curl-7_69_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
737.    return Curl_ssl->random(data, entropy, length);
```

**Use of Insufficiently Random Values\Path 2:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1662 |
| Status | New |

Method Curl_ssl_random at line 762 of curl@@curl-curl-7_71_0-CVE-2021-22924-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_71_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c |
| Line | 766 | 766 |
| Object | random | random |

Code Snippet
File Name curl@@curl-curl-7_71_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
766.    return Curl_ssl->random(data, entropy, length);
```

**Use of Insufficiently Random Values\Path 3:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1663 |
| Status | New |

Method Curl_ssl_random at line 808 of curl@@curl-curl-7_73_0-CVE-2021-22924-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_73_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c |
| Line | 812 | 812 |

| | | |
|---|---|---|
| Object | random | random |

Code Snippet
File Name curl@@curl-curl-7_73_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
812.    return Curl_ssl->random(data, entropy, length);
```

**Use of Insufficiently Random Values\Path 4:**

| | |
|---|---|
| Severity | Low |
| Result State | To Verify |
| Online Results | http://WIN-PTJMSNK3USL/CxWebClient/ViewerMain.aspx?scanid=1000013&projectid=8&pathid=1664 |
| Status | New |

Method Curl_ssl_random at line 814 of curl@@curl-curl-7_75_0-CVE-2021-22924-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_75_0-CVE-2021-22924-TP.c | curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c |
| Line | 818 | 818 |
| Object | random | random |

Code Snippet
File Name curl@@curl-curl-7_75_0-CVE-2021-22924-TP.c
Method CURLcode Curl_ssl_random(struct Curl_easy *data,

```
....
818.    return Curl_ssl->random(data, entropy, length);
```

# 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

# Command Injection

## Risk

### What might happen

An attacker could run arbitrary system-level OS commands on the application server host. Depending on the application's OS permissions, these could include:

- File actions (read / create / modify / delete)
- Open a network connection to the attacker's server
- Start and stop system services
- Modify the running application
- Complete server takeover

---

## Cause

### How does it happen

The application runs an OS system-level command to complete it's task, rather than via the application code. The command includes untrusted data, that may be controllable by an attacker. This untrusted string may contain malicious system-level commands engineered by an attacker, which could be executed as though the attacker were running commands directly on the application server.

In this case, the application receives data from the user input, and passes it as a string to the Operating System. This unvalidated data is then executed by the OS as a system command, running with the same system privileges as the application.

---

## General Recommendations

### How to avoid it

- Refactor the code to avoid any direct shell command execution. Instead, use platform provided APIs or library calls.
- If it is impossible to remove the command execution, execute only static commands that do not include dynamic, user-controlled data.
- Validate all input, regardless of source. Validation should be based on a whitelist: accept only data fitting a specified format, rather than rejecting bad patterns (blacklist). Parameters should be limited to an allowed character set, and non-validated input should be dropped. In addition to characters, check for:
    - Data type
    - Size
    - Range
    - Format
    - Expected values
- In order to minimize damage as a measure of defense in depth, configure the application to run using a restricted user account that has no unnecessary OS privileges.
- If possible, isolate all OS commands to use a separate dedicated user account that has minimal privileges only for the specific commands and files used by the application, according to the Principle of Least Privilege.

- If absolutely necessary to call a system command or execute external program with user input, do not concatenate the user input with the command. Instead, isolate the parameters from the command by using a platform function that supports this.

- Do not call `system()` or it's variants, as this does not support separating data parameters from the system command.
- Instead, use one of the functions that receive arguments separately from the command, and validates them. This includes `ShellExecute()`, `execve()`, or one of it's variants.
- It is very important to pass user-controlled data to the function as the `lpParameters` or `argN` argument (or equivalent), and ensure that it is properly quoted. Never pass user controlled data to as the first parameter for `cmdname` or `filePath`.
- Do not directly execute any shell or command interpreters, such as `bash`, `cmd`, or `make`, with user-controlled input.

---

## Source Code Examples

### CPP

**Execute System (Shell) Command With User Input**

```
int main( int argc, char* argv[] )
{
	int result;
	if ( argc == 2 )
	{
		result = system(argv[1]);
	}
	return result;
}
```

**Call External Program with Safe Parameters**

```
int main( int argc, char* argv[] )
{
	int result;
	if ( argc == 2 )
	{
		char* param = escapeArg(argv[1]);

		result = _spawnl(_P_WAIT, EXTERNAL_PROGRAM_PATH, EXTERNAL_PROGRAM_PATH, param,
NULL);
	}
	return result;
}
```

**Refactor Code to Use API Function**

```
int main( int argc, char* argv[] )
{
	int result;
	if ( argc == 2 )
	{
```

```
            char* param = escapeArg(argv[1]);

            result = performSpecificAction(param);
        }
        return result;
}
```

# Buffer Overflow AddressOfLocalVarReturned

## Risk

### What might happen

A use after free error will cause code to use an area of memory previously assigned with a specific value, which has since been freed and may have been overwritten by another value. This error will likely cause unexpected behavior, memory corruption and crash errors. In some cases where the freed and used section of memory is used to determine execution flow, and the error can be induced by an attacker, this may result in execution of malicious code.

---

## Cause

### How does it happen

Pointers to variables allow code to have an address with a set size to a dynamically allocated variable. Eventually, the pointer's destination may become free - either explicitly in code, such as when programmatically freeing this variable, or implicitly, such as when a local variable is returned - once it is returned, the variable's scope is released. Once freed, this memory will be re-used by the application, overwritten with new data. At this point, dereferencing this pointer will potentially resolve newly written and unexpected data.

---

## General Recommendations

### How to avoid it

- Do not return local variables or pointers
- Review code to ensure no flow allows use of a pointer after it has been explicitly freed

---

## Source Code Examples

### CPP

**Use of Variable after It was Freed**

```
free(input);
printf("%s", input);
```

**Use of Pointer to Local Variable That Was Freed On Return**

```
int* func1()
{
	int i;
	i = 1;
	return &i;
}

void func2()
```

```
{
	int j;
	j = 5;
}

//..
	int * i = func1();
	printf("%d\r\n", *i); // Output could be 1 or Segmentation Fault
	func2();
	printf("%d\r\n", *i); // Output is 5, which is j's value, as func2() overwrote data in
the stack
//..
```

# Buffer Overflow boundcpy WrongSizeParam

## Risk

### What might happen

Buffer overflow attacks, in their various forms, could allow an attacker to control certain areas of memory. Typically, this is used to overwrite data on the stack necessary for the program to function properly, such as code and memory addresses, though other forms of this attack exist. Exploiting this vulnerability can generally lead to system crashes, infinite loops, or even execution of arbitrary code.

---

## Cause

### How does it happen

Buffer Overflows can manifest in numerous different variations. In it's most basic form, the attack controls a buffer, which is then copied to a smaller buffer without size verification. Because the attacker's source buffer is larger than the program's target buffer, the attacker's data overwrites whatever is next on the stack, allowing the attacker to control program structures.
Alternatively, the vulnerability could be the result of improper bounds checking; exposing internal memory addresses outside of their valid scope; allowing the attacker to control the size of the target buffer; or various other forms.

---

## General Recommendations

### How to avoid it

- Always perform proper bounds checking before copying buffers or strings.
- Prefer to use safer functions and structures, e.g. safe string classes over `char*`, `strncpy` over `strcpy`, and so on.
- Consistently apply tests for the size of buffers.
- Do not return variable addresses outside the scope of their variables.

---

## Source Code Examples

### CPP

**Overflowing Buffers**

```
const int BUFFER_SIZE = 10;
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    strcpy(buffer, inputString);
}
```

**Checked Buffers**

```
const int BUFFER_SIZE = 10;
const int MAX_INPUT_SIZE = 256;
```

```
char buffer[BUFFER_SIZE];

void copyStringToBuffer(char* inputString)
{
    if (strnlen(inputString, MAX_INPUT_SIZE) < sizeof(buffer))
    {
        strncpy(buffer, inputString, sizeof(buffer));
    }
}
```

# Off by One Error in Methods

## 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

# 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

```
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<br>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**

```
char* getBlock(int fd) {
char* buf = (char*) malloc(BLOCK_SIZE);
if (!buf) {
return NULL;
}
if (read(fd, buf, BLOCK_SIZE) != BLOCK_SIZE) {

return NULL;
}
```

```
return buf;
}
```

## Example 2

Here the problem is that every time a connection is made, more memory is allocated. So if one just opened up more and more connections, eventually the machine would run out of memory.

*(Bad Code)*

*Example Language:* **C**

```
bar connection(){
foo = malloc(1024);
return foo;
}
endConnection(bar foo) {

free(foo);
}
int main() {

while(1) //thread 1
//On a connection
foo=connection(); //thread 2
//When the connection ends
endConnection(foo)
}
```

### Observed Examples

| Reference | Description |
|---|---|
| CVE-2005-3119 | Memory leak because function does not free() an element of a data structure. |
| CVE-2004-0427 | Memory leak when counter variable is not decremented. |
| CVE-2002-0574 | Memory leak when counter variable is not decremented. |
| CVE-2005-3181 | Kernel uses wrong function to release a data structure, preventing data from being properly tracked by other code. |
| CVE-2004-0222 | Memory leak via unknown manipulations as part of protocol test suite. |
| CVE-2001-0136 | Memory leak via a series of the same command. |

### Potential Mitigations

Pre-design: Use a language or compiler that performs automatic bounds checking.

**Phase: Architecture and Design**

Use an abstraction library to abstract away risky APIs. Not a complete solution.

Pre-design through Build: The Boehm-Demers-Weiser Garbage Collector or valgrind can be used to detect leaks in code. This is not a complete solution as it is not 100% effective.

### Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | **Seven Pernicious Kingdoms (primary)700** |
| ChildOf | Category | 399 | Resource Management Errors | **Development Concepts (primary)699** |
| ChildOf | Category | 633 | Weaknesses that Affect Memory | **Resource-specific Weaknesses (primary)631** |
| ChildOf | Category | 730 | OWASP Top Ten 2004 Category A9 - Denial of Service | **Weaknesses in OWASP Top Ten (2004) (primary)711** |
| ChildOf | Weakness Base | 772 | Missing Release of Resource after Effective | **Research Concepts (primary)1000** |

| | | | | |
|---|---|---|---|---|
| | | | Lifetime | |
| MemberOf | View | 630 | Weaknesses Examined by SAMATE | **Weaknesses Examined by SAMATE (primary)630** |
| CanFollow | Weakness Class | 390 | Detection of Error Condition Without Action | Research Concepts1000 |

## Relationship Notes

This is often a resultant weakness due to improper handling of malformed data or early termination of sessions.

## Affected Resources

- Memory

## Functional Areas

- Memory management

## Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| PLOVER | | | Memory leak |
| 7 Pernicious Kingdoms | | | Memory Leak |
| CLASP | | | Failure to deallocate data |
| OWASP Top Ten 2004 | A9 | CWE More Specific | Denial of Service |

## White Box Definitions

A weakness where the code path has:

1. start statement that allocates dynamically allocated memory resource

2. end statement that loses identity of the dynamically allocated memory resource creating situation where dynamically allocated memory resource is never relinquished

Where "loses" is defined through the following scenarios:

1. identity of the dynamic allocated memory resource never obtained

2. the statement assigns another value to the data element that stored the identity of the dynamically allocated memory resource and there are no aliases of that data element

3. identity of the dynamic allocated memory resource obtained but never passed on to function for memory resource release

4. the data element that stored the identity of the dynamically allocated resource has reached the end of its scope at the statement and there are no aliases of that data element

## References

J. Whittaker and H. Thompson. "How to Break Software Security". Addison Wesley. 2003.

## Content History

| Submissions | | | |
|---|---|---|---|
| **Submission Date** | **Submitter** | **Organization** | **Source** |
| | PLOVER | | Externally Mined |
| **Modifications** | | | |
| **Modification Date** | **Modifier** | **Organization** | **Source** |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-08-15 | | Veracode | External |
| | Suggested OWASP Top Ten 2004 mapping | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Relationships, Other Notes, References, Relationship Notes, Taxonomy Mappings, Terminology Notes | | |
| 2008-10-14 | CWE Content Team | MITRE | Internal |
| | updated Description | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Other Notes | | |
| 2009-05-27 | CWE Content Team | MITRE | Internal |
| | updated Name | | |
| 2009-07-17 | KDM Analytics | | External |
| | Improved the White Box Definition | | |

| | | | |
|---|---|---|---|
| 2009-07-27 | CWE Content Team | MITRE | Internal |
| | updated White Box Definitions | | |
| 2009-10-29 | CWE Content Team | MITRE | Internal |
| | updated Modes of Introduction, Other Notes | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Relationships | | |

**Previous Entry Names**

| Change Date | Previous Entry Name |
|---|---|
| 2008-04-11 | Memory Leak |
| 2009-05-27 | Failure to Release Memory Before Removing Last Reference (aka 'Memory Leak') |

BACK TO TOP

# Use of Zero Initialized Pointer

## Risk

### What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

---

## Cause

### How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

---

## General Recommendations

### How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

---

## Source Code Examples

### CPP

**Explicit NULL Dereference**

```
char * input = NULL;
printf("%s", input);
```

**Implicit NULL Dereference**

```
char * input;
printf("%s", input);
```

### Java

**Explicit Null Dereference**

```
Object o = null;
out.println(o.getClass());
```

## Use of Function with Inconsistent Implementations

**Weakness ID:** 474 *(Weakness Base)* **Status:** Draft

### Description

## Description Summary

The code uses a function that has inconsistent implementations across operating systems and versions, which might cause security-relevant portability problems.

### Time of Introduction

- Architecture and Design
- Implementation

### Applicable Platforms

## Languages

C: *(Often)*

PHP: *(Often)*

All

### Potential Mitigations

Do not accept inconsistent behavior from the API specifications when the deviant behavior increase the risk level.

### Other Notes

The behavior of functions in this category varies by operating system, and at times, even by operating system version. Implementation differences can include:

- Slight differences in the way parameters are interpreted leading to inconsistent results.
- Some implementations of the function carry significant security risks.
- The function might not be defined on all platforms.

### Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Weakness Class | 398 | Indicator of Poor Code Quality | **Development Concepts (primary)699 Seven Pernicious Kingdoms (primary)700 Research Concepts (primary)1000** |
| ParentOf | Weakness Variant | 589 | Call to Non-ubiquitous API | **Research Concepts (primary)1000** |

### Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| 7 Pernicious Kingdoms | | | Inconsistent Implementations |

### Content History

| Submissions | | | |
|---|---|---|---|
| **Submission Date** | **Submitter** | **Organization** | **Source** |
| | 7 Pernicious Kingdoms | | Externally Mined |
| **Modifications** | | | |
| **Modification Date** | **Modifier** | **Organization** | **Source** |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Potential Mitigations, Time of Introduction | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Relationships, Other Notes, Taxonomy Mappings | | |
| **Previous Entry Names** | | | |
| **Change Date** | **Previous Entry Name** | | |
| 2008-04-11 | Inconsistent Implementations | | |

BACK TO TOP

# Use of Insufficiently Random Values

## Risk

### What might happen

Random values are often used as a mechanism to prevent malicious users from guessing a value, such as a password, encryption key, or session identifier. Depending on what this random value is used for, an attacker would be able to predict the next numbers generated, or previously generated values. This could enable the attacker to hijack another user's session, impersonate another user, or crack an encryption key (depending on what the pseudo-random value was used for).

---

## Cause

### How does it happen

The application uses a weak method of generating pseudo-random values, such that other numbers could be determined from a relatively small sample size. Since the pseudo-random number generator used is designed for statistically uniform distribution of values, it is approximately deterministic. Thus, after collecting a few generated values (e.g. by creating a few individual sessions, and collecting the sessionids), it would be possible for an attacker to calculate another sessionid.
Specifically, if this pseudo-random value is used in any security context, such as passwords, keys, or secret identifiers, an attacker would be able to predict the next numbers generated, or previously generated values.

---

## General Recommendations

### How to avoid it

Generic Guidance:

- Whenever unpredicatable numbers are required in a security context, use a cryptographically strong random number generator, instead of a statistical pseudo-random generator.
- Use the cryptorandom generator that is built-in to your language or platform, and ensure it is securely seeded. Do not seed the generator with a weak, non-random seed. (In most cases, the default is securely random).
- Ensure you use a long enough random value, to make brute-force attacks unfeasible.

Specific Recommendations:

- Do not use the statistical pseudo-random number generator, use the cryptorandom generator instead. In Java, this is the SecureRandom class.

---

## Source Code Examples

### Java

**Use of a weak pseudo-random number generator**

```
Random random = new Random();

long sessNum = random.nextLong();

String sessionId = sessNum.toString();
```

```
```

**Cryptographically secure random number generator**

```
SecureRandom random = new SecureRandom();

byte sessBytes[] = new byte[32];

random.nextBytes(sessBytes);

String sessionId = new String(sessBytes);
```

**Objc**

**Use of a weak pseudo-random number generator**

```
long sessNum = rand();
NSString* sessionId = [NSString stringWithFormat:@"%ld", sessNum];
```

**Cryptographically secure random number generator**

```
UInt32 sessBytes;
SecRandomCopyBytes(kSecRandomDefault, sizeof(sessBytes), (uint8_t*)&sessBytes);

NSString* sessionId = [NSString stringWithFormat:@"%llu", sessBytes];
```

**Swift**

**Use of a weak pseudo-random number generator**

```
let sessNum = rand();
let sessionId = String(format:"%ld", sessNum)
```

**Cryptographically secure random number generator**

```
var sessBytes: UInt32 = 0
withUnsafeMutablePointer(&sessBytes, { (sessBytesPointer) -> Void in
    let castedPointer = unsafeBitCast(sessBytesPointer, UnsafeMutablePointer<UInt8>.self)
    SecRandomCopyBytes(kSecRandomDefault, sizeof(UInt32), castedPointer)
})

let sessionId = String(format:"%llu", sessBytes)
```

# Unchecked Return Value

## Risk

### What might happen

A program that does not check function return values could cause the application to enter an undefined state. This could lead to unexpected behavior and unintended consequences, including inconsistent data, system crashes or other error-based exploits.

---

## Cause

### How does it happen

The application calls a system function, but does not receive or check the result of this funciton. These functions often return error codes in the result, or share other status codes with it's caller. The application simply ignores this result value, losing this vital information.

---

## General Recommendations

### How to avoid it

- Always check the result of any called function that returns a value, and verify the result is an expected value.

- Ensure the calling function responds to all possible return values.

- Expect runtime errors and handle them gracefully. Explicitly define a mechanism for handling unexpected errors.

---

## Source Code Examples

### CPP

**Unchecked Memory Allocation**

```
buff = (char*) malloc(size);
strncpy(buff, source, size);
```

**Safer Memory Allocation**

```
buff = (char*) malloc(size+1);
if (buff==NULL) exit(1);

strncpy(buff, source, size);
buff[size] = '\0';
```

## Use of sizeof() on a Pointer Type

**Weakness ID:** 467 *(Weakness Variant)* **Status:** Draft

### Description

### Description Summary

The code calls sizeof() on a malloced pointer type, which always returns the wordsize/8. This can produce an unexpected result if the programmer intended to determine how much memory has been allocated.

### Time of Introduction

- Implementation

### Applicable Platforms

### Languages

C

C++

### Common Consequences

| Scope | Effect |
|---|---|
| Integrity | This error can often cause one to allocate a buffer that is much smaller than what is needed, leading to resultant weaknesses such as buffer overflows. |

### Likelihood of Exploit

High

### Demonstrative Examples

### Example 1

Care should be taken to ensure sizeof returns the size of the data structure itself, and not the size of the pointer to the data structure.

In this example, sizeof(foo) returns the size of the pointer.

*(Bad Code)*

*Example Languages:* **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(foo));
```

In this example, sizeof(*foo) returns the size of the data structure and not the size of the pointer.

*(Good Code)*

*Example Languages:* **C and C++**

```
double *foo;
...
foo = (double *)malloc(sizeof(*foo));
```

### Example 2

This example defines a fixed username and password. The AuthenticateUser() function is intended to accept a username and a password from an untrusted user, and check to ensure that it matches the username and password. If the username and password match, AuthenticateUser() is intended to indicate that authentication succeeded.

*(Bad Code)*

```
/* Ignore CWE-259 (hard-coded password) and CWE-309 (use of password system for authentication) for this example. */

char *username = "admin";
char *pass = "password";

int AuthenticateUser(char *inUser, char *inPass) {
```

```
printf("Sizeof username = %d\n", sizeof(username));
printf("Sizeof pass = %d\n", sizeof(pass));

if (strncmp(username, inUser, sizeof(username))) {
printf("Auth failure of username using sizeof\n");
return(AUTH_FAIL);
}
/* Because of CWE-467, the sizeof returns 4 on many platforms and architectures. */
if (! strncmp(pass, inPass, sizeof(pass))) {
printf("Auth success of password using sizeof\n");
return(AUTH_SUCCESS);
}
else {
printf("Auth fail of password using sizeof\n");
return(AUTH_FAIL);
}
}

int main (int argc, char **argv)
{
int authResult;

if (argc < 3) {
ExitError("Usage: Provide a username and password");
}
authResult = AuthenticateUser(argv[1], argv[2]);
if (authResult != AUTH_SUCCESS) {
ExitError("Authentication failed");
}
else {
DoAuthenticatedTask(argv[1]);
}
}
```

In AuthenticateUser(), because sizeof() is applied to a parameter with an array type, the sizeof() call might return 4 on many modern architectures. As a result, the strncmp() call only checks the first four characters of the input password, resulting in a partial comparison (CWE-187), leading to improper authentication (CWE-287).

Because of the partial comparison, any of these passwords would still cause authentication to succeed for the "admin" user:

*(Attack)*

```
pass5
passABCDEFGH
passWORD
```

Because only 4 characters are checked, this significantly reduces the search space for an attacker, making brute force attacks more feasible.

The same problem also applies to the username, so values such as "adminXYZ" and "administrator" will succeed for the username.

## Potential Mitigations

**Phase: Implementation**

Use expressions such as "sizeof(*pointer)" instead of "sizeof(pointer)", unless you intend to run sizeof() on a pointer type to gain some platform independence or if you are allocating a variable on the stack.

## Other Notes

The use of sizeof() on a pointer can sometimes generate useful information. An obvious case is to find out the wordsize on a platform. More often than not, the appearance of sizeof(pointer) indicates a bug.

## Weakness Ordinalities

| Ordinality | Description |
|---|---|
| Primary | *(where the weakness exists independent of other weaknesses)* |

## Relationships

| Nature | Type | ID | Name | View(s) this relationship pertains to |
|---|---|---|---|---|
| ChildOf | Category | 465 | Pointer Issues | **Development Concepts (primary)699** |
| ChildOf | Weakness Class | 682 | Incorrect Calculation | **Research Concepts (primary)1000** |
| ChildOf | Category | 737 | CERT C Secure Coding Section 03 - Expressions (EXP) | **Weaknesses Addressed by the CERT C Secure Coding Standard (primary)734** |
| ChildOf | Category | 740 | CERT C Secure Coding Section 06 - Arrays (ARR) | Weaknesses Addressed by the CERT C Secure Coding Standard734 |
| CanPrecede | Weakness Base | 131 | Incorrect Calculation of Buffer Size | Research Concepts1000 |

## Taxonomy Mappings

| Mapped Taxonomy Name | Node ID | Fit | Mapped Node Name |
|---|---|---|---|
| CLASP | | | Use of sizeof() on a pointer type |
| CERT C Secure Coding | ARR01-C | | Do not apply the sizeof operator to a pointer when taking the size of an array |
| CERT C Secure Coding | EXP01-C | | Do not take the size of a pointer to determine the size of the pointed-to type |

## White Box Definitions

A weakness where code path has:

1. end statement that passes an identity of a dynamically allocated memory resource to a sizeof operator
2. start statement that allocates the dynamically allocated memory resource

## References

Robert Seacord. "EXP01-A. Do not take the sizeof a pointer to determine the size of a type". <https://www.securecoding.cert.org/confluence/display/seccode/EXP01-A.+Do+not+take+the+sizeof+a+pointer+to+determine+the+size+of+a+type>.

## Content History

| Submissions | | | |
|---|---|---|---|
| **Submission Date** | **Submitter** | **Organization** | **Source** |
| | CLASP | | Externally Mined |
| **Modifications** | | | |
| **Modification Date** | **Modifier** | **Organization** | **Source** |
| 2008-07-01 | Eric Dalci | Cigital | External |
| | updated Time of Introduction | | |
| 2008-08-01 | | KDM Analytics | External |
| | added/updated white box definitions | | |
| 2008-09-08 | CWE Content Team | MITRE | Internal |
| | updated Applicable Platforms, Common Consequences, Relationships, Other Notes, Taxonomy Mappings, Weakness Ordinalities | | |
| 2008-11-24 | CWE Content Team | MITRE | Internal |
| | updated Relationships, Taxonomy Mappings | | |
| 2009-03-10 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2009-12-28 | CWE Content Team | MITRE | Internal |
| | updated Demonstrative Examples | | |
| 2010-02-16 | CWE Content Team | MITRE | Internal |
| | updated Relationships | | |

BACK TO TOP

# Potential Off by One Error in Loops

## Risk

### What might happen

An off by one error may result in overwriting or over-reading of unintended memory; in most cases, this can result in unexpected behavior and even application crashes. In other cases, where allocation can be controlled by an attacker, a combination of variable assignment and an off by one error can result in execution of malicious code.

---

## Cause

### How does it happen

Often when designating variables to memory, a calculation error may occur when determining size or length that is off by one.

For example in loops, when allocating an array of size 2, its cells are counted as 0,1 - therefore, if a For loop iterator on the array is incorrectly set with the start condition i=0 and the continuation condition i<=2, three cells will be accessed instead of 2, and an attempt will be made to write or read cell [2], which was not originally allocated, resulting in potential corruption of memory outside the bounds of the originally assigned array.

Another example occurs when a null-byte terminated string, in the form of a character array, is copied without its terminating null-byte. Without the null-byte, the string representation is unterminated, resulting in certain functions to over-read memory as they expect the missing null terminator.

---

## General Recommendations

### How to avoid it

- Always ensure that a given iteration boundary is correct:
  - With array iterations, consider that arrays begin with cell 0 and end with cell n-1, for a size n array.
  - With character arrays and null-byte terminated string representations, consider that the null byte is required and should not be overwritten or ignored; ensure functions in use are not vulnerable to off-by-one, specifically for instances where null-bytes are automatically appended after the buffer, instead of in place of its last character.
- Where possible, use safe functions that manage memory and are not prone to off-by-one errors.

---

## Source Code Examples

### CPP

### Off-By-One in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i <= 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[5] will be set, but is out of bounds
```

```
}
```

### Proper Iteration in For Loop

```
int *ptr;
ptr = (int*)malloc(5 * sizeof(int));
for (int i = 0; i < 5; i++)
{
      ptr[i] = i * 2 + 1; // ptr[0-4] are well defined
}
```

### Off-By-One in strncat

```
strncat(buf, input, sizeof(buf) - strlen(buf)); // actual value should be sizeof(buf)-
strlen(buf)-1 - this form will overwrite the terminating nullbyte
```

# NULL Pointer Dereference

## Risk

### What might happen

A null pointer dereference is likely to cause a run-time exception, a crash, or other unexpected behavior.

## Cause

### How does it happen

Variables which are declared without being assigned will implicitly retain a null value until they are assigned. The null value can also be explicitly set to a variable, to ensure clear out its contents. Since null is not really a value, it may not have object variables and methods, and any attempt to access contents of a null object, instead of verifying it is set beforehand, will result in a null pointer dereference exception.

## General Recommendations

### How to avoid it

- For any variable that is created, ensure all logic flows between declaration and use assign a non-null value to the variable first.
- Enforce null checks on any received variable or object before it is dereferenced, to ensure it does not contain a null assigned to it elsewhere.
- Consider the need to assign null values in order to overwrite initialized variables. Consider reassigning or releasing these variables instead.

## Source Code Examples

## 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 {
    //[..]
};
```

# 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--;
       }
    }
}
```

## 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

## 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<br>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<br>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<br>Availability<br>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 |